

CONSTRUCTION OF UNIPOTENT GALOIS EXTENSIONS AND MASSEY PRODUCTS

JÁN MINÁČ AND NGUYỄN DUY TÂN

Dedicated to Alexander Merkurjev

ABSTRACT. For all primes p and for all fields, we find a sufficient and necessary condition of the existence of a unipotent Galois extension of degree p^6 . The main goal of this paper is to describe an explicit construction of such a Galois extension over fields admitting such a Galois extension. This construction is surprising in its simplicity and generality. The problem of finding such a construction has been left open since 2003. Recently a possible solution of this problem gained urgency because of an effort to extend new advances in Galois theory and its relations with Massey products in Galois cohomology.

1. INTRODUCTION

From the very beginning of the invention of Galois theory, one problem has emerged. For a given finite group G , find a Galois extension K/\mathbb{Q} such that $\text{Gal}(K/\mathbb{Q}) \simeq G$. This is still an open problem in spite of the great efforts of a number of mathematicians and substantial progress having been made with specific groups G . (See [Se3].) A more general problem is to ask the same question over other base fields F . This is a challenging and difficult problem even for groups G of prime power order.

In this paper we make progress on this classical problem in Galois theory. Moreover this progress fits together well with a new development relating Massey products in Galois cohomology to basic problems in Galois theory. For all primes p and all fields in the key test case of $n = 4$, we construct Galois extensions with the unipotent Galois group $\mathbb{U}_n(\mathbb{F}_p)$ assuming only the existence of some Galois extensions of order p^3 . This fits into a program outlined in [MT1] and [MT2], for the systematic construction of Galois p -closed extensions of general fields, assuming only knowledge of Galois extensions of degree less than or equal to p^3 and the structure of p th power roots of unity in the base field. Thus both the methods and the results in this paper pave the way to a program for obtaining the structure of maximal pro- p -quotients of absolute Galois groups for all fields. We shall now describe some previous work of a number of mathematicians which has influenced our work, as well as its significance for further developments and applications.

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. NDT is partially supported by the National Foundation for Science and Technology Development (NAFOSTED) grant 101.04-2014.34.

Recently there has been substantial progress in Galois cohomology which has changed our perspective on Galois p -extensions over general fields. In some remarkable work, M. Rost and V. Voevodsky proved the Bloch-Kato conjecture on the structure of Galois cohomology of general fields. (See [Voe1, Voe2].) From this work it follows that there must be enough Galois extensions to make higher degree Galois cohomology decomposable. However the explicit construction of such Galois extensions is completely mysterious. In [MT1], [MT2] and [MT5], two new conjectures, the Vanishing n -Massey Conjecture and the Kernel n -Unipotent Conjecture were proposed. These conjectures in [MT1] and [MT2], and the results in this paper, lead to a program of constructing these previously mysterious Galois extensions in a systematic way. In these papers it is shown that the truth of these conjectures has some significant implications on the structure of absolute Galois groups. These conjectures are based on a number of previous considerations. One motivation comes from topological considerations. (See [DGMS] and [HW].) Another motivation is a program to describe various n -central series of absolute Galois groups as kernels of simple Galois representations. (See [CEM, Ef, EM1, EM2, MSp, NQD, Vi].) If the Vanishing n -Massey Conjecture is true, then by a result in [Dwy], we obtain a program of building up n -unipotent Galois representations of absolute Galois groups by induction on n . This is an attractive program because we obtain a procedure of constructing larger Galois p -extensions from smaller ones, efficiently using the fact that certain *a priori* natural cohomological obstructions to this procedure always vanish.

Recall that for each natural number n , $\mathbb{U}_n(\mathbb{F}_p)$ is the group of upper triangular $n \times n$ -matrices with entries in \mathbb{F}_p and diagonal entries 1. Then $\mathbb{U}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8, and if p is odd, then $\mathbb{U}_3(\mathbb{F}_p)$ is isomorphic to the Heisenberg group H_{p^3} of order p^3 . For all $n \geq 4$ and all primes p , we can think of $\mathbb{U}_n(\mathbb{F}_p)$ as "higher Heisenberg groups" of order $p^{n(n-1)/2}$. It is now recognized that these groups play a very special role in current Galois theory. Because $\mathbb{U}_n(\mathbb{F}_p)$ is a Sylow p -subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, and every finite p -group has a faithful linear n -dimensional representation over \mathbb{F}_p , for some n , we see that every finite p -group can be embedded into $\mathbb{U}_n(\mathbb{F}_p)$ for some n . Besides, the Vanishing n -Massey Conjecture and the Kernel n -Unipotent Conjecture also indicate some deeper reasons why $\mathbb{U}_n(\mathbb{F}_p)$ is of special interest. The constructions of Galois extensions with the Galois group $\mathbb{U}_3(\mathbb{F}_p)$ over fields which admit them, are well-known in the case when the base field is of characteristic not p . They are an important basic tool in the Galois theory of p -extensions. (See for example [JLY, Sections 6.5 and 6.6]. Some early papers related to these topics like [MNg] and [M] now belong to classical work on Galois theory.)

In [GLMS, Section 4], a construction of Galois extensions K/F , $\mathrm{char}(F) \neq 2$, with $\mathrm{Gal}(K/F) \simeq \mathbb{U}_4(\mathbb{F}_2)$, was discovered. Already at that time, one reason for searching for this construction was the motivation to find ideas to extend deep results on the characterization of the fixed field of the third 2-Zassenhaus filtration of an absolute Galois group G_F as the compositum of Galois extensions of degree at most 8 (see

[Ef, EM2, MSp, Vi]), to a similar characterization of the fixed field of the fourth 2-Zassenhaus filtration of G_F . In retrospect, looking at this construction, one recognizes some elements of the basic theory of Massey products. However at that time the authors of [GLMS] were not familiar with Massey products. It was realized that such a construction would also be desirable for $\mathbb{U}_4(\mathbb{F}_p)$ for all p rather than $\mathbb{U}_4(\mathbb{F}_2)$, but none has been found until now.

In [GLMS], in the construction of a Galois field extension K/F with $\text{Gal}(K/F) \simeq \mathbb{U}_4(\mathbb{F}_2)$, a simple criteria was used for an element in F to be a norm from a bicyclic extension of degree 4 modulo non-zero squares in the base field F . However in [Me], A. Merkurjev showed that a straightforward generalization of this criteria for p odd instead of $p = 2$, is not true in general. Therefore it was not clear whether such an analogous construction of Galois extensions K/F with $\text{Gal}(K/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$ was possible for p odd.

On the other hand, a new consideration in [HW], [MT1] and [MT2] led us to formulate the Vanishing n -Massey Conjecture, and the most natural way to prove this conjecture for $n = 3$ in the key non-degenerate case would be through constructing explicit Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions. In fact we pursued both cohomological variants of proving the Vanishing 3-Massey Conjecture and the Galois theoretic construction of Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions.

The story of proving this conjecture and finally constructing Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions over all fields which admit them, is interesting. First M. J. Hopkins and K. G. Wickelgren in [HW] proved a result which implies that the Vanishing 3-Massey Conjecture with respect to prime 2, is true for all global fields of characteristic not 2. In [MT1] we proved that the result of [HW] is valid for any field F . At the same time, in [MT1] the Vanishing n -Massey Conjecture was formulated, and applications on the structure of the quotients of absolute Galois groups were deduced. In [MT3] we proved that the Vanishing 3-Massey Conjecture with respect to any prime p is true for any global field F containing a primitive p -th root of unity. In [EMa1], I. Efrat and E. Matzri provided alternative proofs for the above-mentioned results in [MT1] and [MT3]. In [Ma], E. Matzri proved that for any prime p and for any field F containing a primitive p -th root of unity, every defined triple Massey product contains 0. This established the Vanishing 3-Massey Conjecture in the form formulated in [MT1]. Shortly after [Ma] appeared on the arXiv, two new preprints, [EMa2] and [MT5], appeared nearly simultaneously and independently on the arXiv as well. In [EMa2], I. Efrat and E. Matzri replace [Ma] and provide a cohomological approach to the proof of the main result in [Ma]. In [MT5] we also provide a cohomological method of proving the same result. We also extend the vanishing of triple Massey products to all fields, and thus remove the restriction that the base field contains a primitive p -th root of unity. We further provide applications on the structure of some canonical quotients of absolute Galois groups, and also show that some special higher n -fold Massey products vanish. Finally in this paper we are able to provide a construction of the Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension M/F for any field F which admits such an extension. We use this construction to provide a natural new proof, which

we were seeking from the beginning of our search for a Galois theoretic proof, of the vanishing of triple Massey products over all fields.

Some interesting cases of "automatic" realizations of Galois groups are known. These are cases when the existence of one Galois group over a given field forces the existence of some other Galois groups over this field. (See for example [Je, MS2, MSS, MZ, Wh].) However, nontrivial cases of automatic realizations coming from an actual construction of embedding smaller Galois extensions to larger ones, are relatively rare, and they are difficult to produce. In our construction we are able, from knowledge of the existence of two Heisenberg Galois extensions of degree p^3 over a given base field F as above, to find possibly another pair of Heisenberg Galois extensions whose compositum can be automatically embedded in a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension. (See also Remark 3.3.) Observe that in all proofs of the Vanishing 3-Massey Conjecture we currently have, constructing Heisenberg Galois extensions of degree p^3 has played an important role. For the sake of a possible inductive proof of the Vanishing n -Massey Conjecture, it seems important to be able to inductively construct Galois $\mathbb{U}_n(\mathbb{F}_p)$ -extensions. This has now been achieved for the induction step from $n = 3$ to $n = 4$, and it opens up a way to approach the Vanishing 4-Massey Conjecture.

Another motivation for this work which combines well with the motivation described above, comes from anabelian birational considerations. Very roughly in various generality and precision, it was observed that small canonical quotients of absolute Galois groups determine surprisingly precise information about base fields, in some cases entire base fields up to isomorphisms. (See [BT1, BT2, CEM, EM1, EM2, MSp, Pop].) But these results suggest that some small canonical quotients of an absolute Galois group together with knowledge of the roots of unity in the base field should determine larger canonical quotients of this absolute Galois group. The Vanishing n -Massey Conjecture and the Kernel n -Unipotent Conjecture, together with the program of explicit constructions of Galois $\mathbb{U}_n(\mathbb{F}_p)$ -extensions, make this project more precise. Thus our main results, Theorems 3.7, 3.9, 4.3 and 5.5, contribute to this project.

A further potentially important application for this work is the theory of Galois p -extensions of global fields with restricted ramification and questions surrounding the Fontaine-Mazur conjecture. (See [Ko], [La], [McL], [Ga],[Se2].) For example in [McL, Section 3], there is a criterion for infinite Hilbert p -class field towers over quadratic imaginary number fields relying on the vanishing of certain triple Massey products. The explicit constructions in this paper should be useful for approaching these classical number theoretic problems.

Only relatively recently, the investigations of the Galois realizability of some larger p -groups among families of small p -groups, appeared. (See the very interesting papers [Mi1], [Mi2], [GS].) In these papers the main concern is understanding cohomological and Brauer group obstructions for the realizability of Galois field extensions with prescribed Galois groups. In our paper the main concern is the explicit constructions and their connections with Massey products. In other recent papers [CMS] and [Sch], the

authors succeeded to treat the cases of characteristic equal to p or not equal to p , nearly uniformly. This is also the case with our paper.

Our paper is organized as follows. In Section 2 we recall basic notions about norm residue symbols and Heisenberg extensions of degree p^3 . (For convenience we think of the dihedral group of order 8 as the Heisenberg group of order 8.) In Section 3 we provide a detailed construction of Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions beginning with two "compatible" Heisenberg extensions of degree p^3 . Section 3 is divided into two subsections. In Subsection 3.1 we provide a construction of the required Galois extension M/F over any field F which contains a primitive p -th root of unity. In Subsection 3.2 we provide such a construction for all fields of characteristic not p , building on the results and methods in Subsection 3.1. In Example 3.8 we illustrate our method on a surprisingly simple construction of Galois $\mathbb{U}_4(\mathbb{F}_2)$ -extensions over any field F with $\text{char}(F) \neq 2$. In Section 4 we provide a required construction for all fields of characteristic p . After the original and classical papers of E. Artin and O. Schreier [ASch] and E. Witt [Wi], these constructions seem to add new results on the construction of basic Galois extensions M/F with Galois groups $\mathbb{U}_n(\mathbb{F}_p)$, $n = 3$ and $n = 4$. These are aesthetically pleasing constructions with remarkable simplicity. They follow constructions in characteristic not p , but they are simpler. See also [JLY, Section 5.6 and Appendix A1] for another procedure to obtain these Galois extensions. In Section 5 we provide a new natural Galois theoretic proof of the vanishing of triple Massey products over all fields in the key non-degenerate case. We also complete the new proof of the vanishing of triple Massey products in the case when a primitive p -th root of unity is contained in the base field. Finally we formulate a necessary and sufficient condition for the existence of a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension M/F which contains an elementary p -extension of any field F (described by three linearly independent characters), and we summarize the main results in Theorem 5.5.

Acknowledgements: We would like to thank M. Ataei, L. Bary-Soroker, S. K. Chebolu, I. Efrat, H. Ésnault, E. Frenkel, S. Gille, J. Gärtner, P. Guillot, D. Harbater, M. J. Hopkins, Ch. Kapulkin, I. Kříž, J. Labute, T.-Y. Lam, Ch. Maire, E. Matzri, C. McLeman, D. Neftin, J. Nekovář, R. Parimala, C. Quadrelli, M. Rogelstad, A. Schultz, R. Sujatha, Ng. Q. Th  ng, A. Topaz, K. G. Wickelgren and O. Wittenberg for having been able to share our enthusiasm for this relatively new subject of Massey products in Galois cohomology, and for their encouragement, support, and inspiring discussions. We are very grateful to the anonymous referee for his/her careful reading of our paper, and for providing us with insightful comments and valuable suggestions which we used to improve our exposition.

Notation: If G is a group and $x, y \in G$, then $[x, y]$ denotes the commutator $xyx^{-1}y^{-1}$. For any element σ of finite order n in G , we denote N_σ to be the element $1 + \sigma + \cdots + \sigma^{n-1}$ in the integral group ring $\mathbb{Z}[G]$ of G .

For a field F , we denote F_s (respectively G_F) to be its separable closure (respectively its absolute Galois group $\text{Gal}(F_s/F)$). We denote F^\times to be the set of non-zero elements of

F . For a given profinite group G , we call a Galois extension E/F , a (Galois) G -extension if the Galois group $\text{Gal}(E/F)$ is isomorphic to G .

For a unital commutative ring R and an integer $n \geq 2$, we denote $\mathbb{U}_n(R)$ as the group of all upper-triangular unipotent $n \times n$ -matrices with entries in R . For any (continuous) representation $\rho: G \rightarrow \mathbb{U}_n(R)$ from a (profinite) group G to $\mathbb{U}_n(R)$ (equipped with discrete topology), and $1 \leq i < j \leq n$, let $\rho_{ij}: G \rightarrow R$ be the composition of ρ with the projection from $\mathbb{U}_n(R)$ to its (i, j) -coordinate.

2. HEISENBERG EXTENSIONS

The materials in this section have been taken from [MT5, Section 3].

2.1. Norm residue symbols. Let F be a field containing a primitive p -th root of unity ξ . For any element a in F^\times , we shall write χ_a for the character corresponding to a via the Kummer map $F^\times \rightarrow H^1(G_F, \mathbb{Z}/p\mathbb{Z}) = \text{Hom}(G_F, \mathbb{Z}/p\mathbb{Z})$. From now on we assume that a is not in $(F^\times)^p$. The extension $F(\sqrt[p]{a})/F$ is a Galois extension with the Galois group $\langle \sigma_a \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, where σ_a satisfies $\sigma_a(\sqrt[p]{a}) = \xi \sqrt[p]{a}$.

The character χ_a defines a homomorphism $\chi^a \in \text{Hom}(G_F, \frac{1}{p}\mathbb{Z}/\mathbb{Z}) \subseteq \text{Hom}(G_F, \mathbb{Q}/\mathbb{Z})$ by the formula

$$\chi^a = \frac{1}{p} \chi_a.$$

Let b be any element in F^\times . Then the norm residue symbol may be defined as

$$(a, b) := (\chi^a, b) := b \cup \delta \chi^a.$$

Here δ is the coboundary homomorphism $\delta: H^1(G, \mathbb{Q}/\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z})$ associated to the short exact sequence of trivial G -modules

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

The cup product $\chi_a \cup \chi_b \in H^2(G_F, \mathbb{Z}/p\mathbb{Z})$ can be interpreted as the norm residue symbol (a, b) . More precisely, we consider the exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow F_s^\times \xrightarrow{x \mapsto x^p} F_s^\times \longrightarrow 1,$$

where $\mathbb{Z}/p\mathbb{Z}$ has been identified with the group of p -th roots of unity μ_p via the choice of ξ . As $H^1(G_F, F_s^\times) = 0$, we obtain

$$0 \longrightarrow H^2(G_F, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{i} H^2(G_F, F_s^\times) \xrightarrow{\times p} H^2(G_F, F_s^\times).$$

Then one has $i(\chi_a \cup \chi_b) = (a, b) \in H^2(G_F, F_s^\times)$. (See [Se1, Chapter XIV, Proposition 5].)

2.2. Heisenberg extensions. In this subsection we recall some basic facts about Heisenberg extensions. (See [Sha, Chapter 2, Section 2.4] and [JLY, Sections 6.5 and 6.6].)

Assume that a, b are elements in F^\times , which are linearly independent modulo $(F^\times)^p$. Let $K = F(\sqrt[p]{a}, \sqrt[p]{b})$. Then K/F is a Galois extension whose Galois group is generated by σ_a and σ_b . Here $\sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}$, $\sigma_a(\sqrt[p]{a}) = \xi \sqrt[p]{a}$; $\sigma_b(\sqrt[p]{a}) = \sqrt[p]{a}$, $\sigma_b(\sqrt[p]{b}) = \xi \sqrt[p]{b}$.

We consider a map $\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^2$ which sends $\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}$ to (x, y) . Then we have the following embedding problem

$$\begin{array}{c} G_F \\ \downarrow \bar{\rho} \\ 0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow 1, \end{array}$$

where $\bar{\rho}$ is the map $(\chi_a, \chi_b): G_F \rightarrow \text{Gal}(K/F) \simeq (\mathbb{Z}/p\mathbb{Z})^2$. (The last isomorphism $\text{Gal}(K/F) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ is the one which sends σ_a to $(1, 0)$ and σ_b to $(0, 1)$.)

Assume that $\chi_a \cup \chi_b = 0$. Then the norm residue symbol (a, b) is trivial. Hence there exists α in $F(\sqrt[p]{a})$ such that $N_{F(\sqrt[p]{a})/F}(\alpha) = b$ (see [Se1, Chapter XIV, Proposition 4 (iii)]). We set

$$A_0 = \alpha^{p-1} \sigma_a(\alpha^{p-2}) \cdots \sigma_a^{p-2}(\alpha) = \prod_{i=0}^{p-2} \sigma_a^i(\alpha^{p-i-1}) \in F(\sqrt[p]{a}).$$

Lemma 2.1. *Let f_a be an element in F^\times . Let $A = f_a A_0$. Then we have*

$$\frac{\sigma_a(A)}{A} = \frac{N_{F(\sqrt[p]{a})/F}(\alpha)}{\alpha^p} = \frac{b}{\alpha^p}.$$

Proof. Observe that $\frac{\sigma_a(A)}{A} = \frac{\sigma_a(A_0)}{A_0}$. The lemma then follows from the identity

$$(s-1) \sum_{i=0}^{p-2} (p-i-1)s^i = \sum_{i=0}^{p-1} s^i - ps^0. \quad \square$$

Proposition 2.2. *Assume that $\chi_a \cup \chi_b = 0$. Let f_a be an element in F^\times . Let $A = f_a A_0$ be defined as above. Then the homomorphism $\bar{\rho} := (\chi_a, \chi_b): G_F \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ lifts to a Heisenberg extension $\rho: G_F \rightarrow \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$.*

Sketch of Proof. Let $L := K(\sqrt[p]{A})/F$. Then L/F is Galois extension. Let $\tilde{\sigma}_a \in \text{Gal}(L/F)$ (resp. $\tilde{\sigma}_b \in \text{Gal}(L/F)$) be an extension of σ_a (resp. σ_b). Since $\sigma_b(A) = A$, we have $\tilde{\sigma}_b(\sqrt[p]{A}) = \xi^j \sqrt[p]{A}$, for some $j \in \mathbb{Z}$. Hence $\tilde{\sigma}_b^p(\sqrt[p]{A}) = \sqrt[p]{A}$. This implies that $\tilde{\sigma}_b$ is of order p .

On the other hand, we have $\tilde{\sigma}_a(\sqrt[p]{A})^p = \sigma_a(A) = A \frac{b}{\alpha^p}$. Hence $\tilde{\sigma}_a(\sqrt[p]{A}) = \xi^i \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha}$, for some $i \in \mathbb{Z}$. Then $\tilde{\sigma}_a^p(\sqrt[p]{A}) = \sqrt[p]{A}$. Thus $\tilde{\sigma}_a$ is of order p .

If we set $\sigma_A := [\tilde{\sigma}_a, \tilde{\sigma}_b]$, then $\sigma_A(\sqrt[p]{A}) = \zeta^{-1}\sqrt[p]{A}$. This implies that σ_A is of order p . Also one can check that

$$[\tilde{\sigma}_a, \sigma_A] = [\tilde{\sigma}_b, \sigma_A] = 1.$$

We can define an isomorphism $\varphi: \text{Gal}(L/F) \rightarrow \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ by letting

$$\sigma_a \mapsto \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \sigma_b \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \sigma_A \mapsto \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then the composition $\rho: G_F \rightarrow \text{Gal}(L/F) \xrightarrow{\varphi} \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ is the desired lifting of $\bar{\rho}$.

Note that $[L : F] = p^3$. Hence there are exactly p extensions of $\sigma_a \in \text{Gal}(E/F)$ to the automorphisms in $\text{Gal}(L/F)$ since $[L : E] = p^3/p^2 = p$. Therefore for later use, we can choose an extension, still denoted by $\sigma_a \in \text{Gal}(L/F)$, of $\sigma_a \in \text{Gal}(K/F)$ in such a way that $\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha}$. \square

3. THE CONSTRUCTION OF $\mathbb{U}_4(\mathbb{F}_p)$ -EXTENSIONS: THE CASE OF CHARACTERISTIC $\neq p$

3.1. Fields containing primitive p -th roots of unity. In this subsection we assume that F is a field containing a primitive p -th root ζ of unity. The following result can be deduced from Theorem 5.5, but for the convenience of the reader we include a proof here.

Proposition 3.1. *Assume that there exists a Galois extension M/F such that $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. Then there exist $a, b, c \in F^\times$ such that a, b, c are linearly independent modulo $(F^\times)^p$ and $(a, b) = (b, c) = 0$. Moreover M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$.*

Proof. Let ρ be the composite $\rho: G_F \twoheadrightarrow \text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. Then ρ_{12}, ρ_{23} and ρ_{34} are elements in $\text{Hom}(G_F, \mathbb{F}_p)$. Hence there are a, b and c in F^\times such that $\chi_a = \rho_{12}$, $\chi_b = \rho_{23}$ and $\chi_c = \rho_{34}$. Since ρ is a group homomorphism, by looking at the coboundaries of ρ_{13} and ρ_{24} , we see that

$$\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0 \in H^2(G_F, \mathbb{F}_p).$$

This implies that $(a, b) = (b, c) = 0$ by [Se1, Chapter XIV, Proposition 5].

Let $\varphi := (\chi_a, \chi_b, \chi_c): G_F \rightarrow (\mathbb{F}_p)^3$. Then φ is surjective. By Galois correspondence, we have

$$\text{Gal}(F_s/F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})) = \ker \chi_a \cap \ker \chi_b \cap \ker \chi_c = \ker \varphi.$$

This implies that $\text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F) \simeq (\mathbb{F}_p)^3$. Hence by Kummer theory, we see that a, b and c are linearly independent modulo $(F^\times)^p$. Clearly, M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$. \square

Conversely we shall see in this section that given these necessary conditions for the existence of $\mathbb{U}_4(\mathbb{F}_p)$ -Galois extensions over F , as in Proposition 3.1, we can construct a Galois extension M/F with the Galois group isomorphic to $\mathbb{U}_4(\mathbb{F}_p)$.

From now on we assume that we are given elements a, b and c in F^\times such that a, b and c are linearly independent modulo $(F^\times)^p$ and that $(a, b) = (b, c) = 0$. We shall construct a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension M/F such that M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$.

First we note that $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F$ is a Galois extension with $\text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$ generated by $\sigma_a, \sigma_b, \sigma_c$. Here

$$\begin{aligned}\sigma_a(\sqrt[p]{a}) &= \xi \sqrt[p]{a}, \sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}, \sigma_a(\sqrt[p]{c}) = \sqrt[p]{c}; \\ \sigma_b(\sqrt[p]{a}) &= \sqrt[p]{a}, \sigma_b(\sqrt[p]{b}) = \xi \sqrt[p]{b}, \sigma_b(\sqrt[p]{c}) = \sqrt[p]{c}; \\ \sigma_c(\sqrt[p]{a}) &= \sqrt[p]{a}, \sigma_c(\sqrt[p]{b}) = \sqrt[p]{b}, \sigma_c(\sqrt[p]{c}) = \xi \sqrt[p]{c}.\end{aligned}$$

Let $E = F(\sqrt[p]{a}, \sqrt[p]{c})$. Since $(a, b) = (b, c) = 0$, there are α in $F(\sqrt[p]{a})$ and γ in $F(\sqrt[p]{c})$ (see [Se1, Chapter XIV, Proposition 4 (iii)]) such that

$$N_{F(\sqrt[p]{a})/F}(\alpha) = b = N_{F(\sqrt[p]{c})/F}(\gamma).$$

Let G be the Galois group $\text{Gal}(E/F)$. Then $G = \langle \sigma_a, \sigma_c \rangle$, where $\sigma_a \in G$ (respectively $\sigma_c \in G$) is the restriction of $\sigma_a \in \text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$ (respectively $\sigma_c \in \text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$).

Our next goal is to find an element δ in E^\times such that the Galois closure of $E(\sqrt[p]{\delta})$ is our desired $\mathbb{U}_4(\mathbb{F}_p)$ -extension of F . We define

$$C_0 = \prod_{i=0}^{p-2} \sigma_c^i(\gamma^{p-i-1}) \in F(\sqrt[p]{a}),$$

and define $B := \gamma/\alpha$. Then we have the following result, which follows from Lemma 2.1 (see [Ma, Proposition 3.2] and/or [MT5, Lemma 4.2]).

Lemma 3.2. *We have*

$$\begin{aligned}(1) \quad \frac{\sigma_a(A_0)}{A_0} &= N_{\sigma_c}(B). \\ (2) \quad \frac{\sigma_c(C_0)}{C_0} &= N_{\sigma_a}(B)^{-1}.\end{aligned}$$

□

Remark 3.3. We would like to informally explain the meaning of the next lemma. From our hypothesis $(a, b) = 0 = (b, c)$ and from Subsection 2.2, we see that we can obtain two Heisenberg extensions $L_1 = F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{A_0})$ and $L_2 = F(\sqrt[p]{b}, \sqrt[p]{c}, \sqrt[p]{C_0})$ of F . Here we have chosen specific elements $A_0 \in F(\sqrt[p]{a})$ and $C_0 \in F(\sqrt[p]{c})$. However we may not be able to embed the compositum of L_1 and L_2 into our desired Galois extension M/F with $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. We know that we can modify the element A_0 by any element $f_a \in F^\times$ and the element C_0 by any element $f_c \in F^\times$ obtaining elements $A = f_a A_0$ and $C = f_c C_0$ instead of A_0 and C_0 . This new choice of elements may change the fields L_1 and L_2 but the new fields will still be Heisenberg extensions containing $F(\sqrt[p]{a}, \sqrt[p]{b})$ and $F(\sqrt[p]{b}, \sqrt[p]{c})$ respectively. The next lemma will provide us with a suitable modification of A_0 and C_0 . From the proof of Theorem 3.7 we shall see that the compositum of

these modified Heisenberg extensions can indeed be embedded into a Galois extension M/F with $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. This explains our comment in the introduction in the paragraph related to the "automatic realization of Galois groups".

Lemma 3.4. *Assume that there exist $C_1, C_2 \in E^\times$ such that*

$$B = \frac{\sigma_a(C_1)}{C_1} \frac{C_2}{\sigma_c(C_2)}.$$

Then $N_{\sigma_c}(C_1)/A_0$ and $N_{\sigma_a}(C_2)/C_0$ are in F^\times . Moreover, if we let $A = N_{\sigma_c}(C_1) \in F(\sqrt[p]{a})^\times$ and $C = N_{\sigma_a}(C_2) \in F(\sqrt[p]{c})^\times$, then there exists $\delta \in E^\times$ such that

$$\begin{aligned} \frac{\sigma_c(\delta)}{\delta} &= AC_1^{-p}, \\ \frac{\sigma_a(\delta)}{\delta} &= CC_2^{-p}. \end{aligned}$$

Proof. By Lemma 3.2, we have

$$\frac{\sigma_a(A_0)}{A_0} = N_{\sigma_c}(B) = N_{\sigma_c} \left(\frac{\sigma_a(C_1)}{C_1} \right) N_{\sigma_c} \left(\frac{C_2}{\sigma_c(C_2)} \right) = \frac{\sigma_a(N_{\sigma_c}(C_1))}{N_{\sigma_c}(C_1)}.$$

This implies that

$$\frac{N_{\sigma_c}(C_1)}{A_0} = \sigma_a \left(\frac{N_{\sigma_c}(C_1)}{A_0} \right).$$

Hence

$$\frac{N_{\sigma_c}(C_1)}{A_0} \in F(\sqrt[p]{c})^\times \cap F(\sqrt[p]{a})^\times = F^\times.$$

By Lemma 3.2, we have

$$\frac{\sigma_c(C_0)}{C_0} = N_{\sigma_a}(B^{-1}) = N_{\sigma_a} \left(\frac{C_1}{\sigma_a(C_1)} \right) N_{\sigma_a} \left(\frac{\sigma_c(C_2)}{C_2} \right) = \frac{\sigma_c(N_{\sigma_a}(C_2))}{N_{\sigma_a}(C_2)}.$$

This implies that

$$\frac{N_{\sigma_a}(C_2)}{C_0} = \sigma_c \left(\frac{N_{\sigma_a}(C_2)}{C_0} \right).$$

Hence

$$\frac{N_{\sigma_a}(C_2)}{C_0} \in F(\sqrt[p]{a})^\times \cap F(\sqrt[p]{c})^\times = F^\times.$$

Clearly, one has

$$\begin{aligned} N_{\sigma_a}(CC_2^{-p}) &= 1, \\ N_{\sigma_c}(AC_1^{-p}) &= 1. \end{aligned}$$

We also have

$$\begin{aligned} \frac{\sigma_a(AC_1^{-p})}{AC_1^{-p}} \frac{CC_2^{-p}}{\sigma_c(CC_2^{-p})} &= \frac{\sigma_a(A)}{A} \left(\frac{\sigma_a(C_1)}{C_1} \right)^{-p} \frac{C}{\sigma_c(C)} \left(\frac{C_2}{\sigma_c(C_2)} \right)^{-p} \\ &= \frac{b}{\alpha^p} \frac{\gamma^p}{b} B^{-p} \\ &= 1. \end{aligned}$$

Hence, we have

$$\frac{\sigma_a(AC_1^{-p})}{AC_1^{-p}} = \frac{\sigma_c(CC_2^{-p})}{CC_2^{-p}}.$$

From [Co, page 756] we see that there exists $\delta \in E^\times$ such that

$$\begin{aligned} \frac{\sigma_c(\delta)}{\delta} &= AC_1^{-p}, \\ \frac{\sigma_a(\delta)}{\delta} &= CC_2^{-p}, \end{aligned}$$

as desired. \square

Remark 3.5. The result of I. G. Connell which we use in the above proof, is a variant of Hilbert's Theorem 90. This result was independently discovered by S. Amitsur and D. Saltman in [AS, Lemma 2.4]. (See also [DMSS, Theorem 2] for the case $p = 2$.)

Lemma 3.6. *There exists $e \in E^\times$ such that $B = \frac{\sigma_a \sigma_c(e)}{e}$. Furthermore, for such an element e the following statements are true.*

- (1) *If we set $C_1 := \sigma_c(e) \in E^\times$, $C_2 := e^{-1} \in E^\times$, then $B = \frac{\sigma_a(C_1)}{C_1} \frac{C_2}{\sigma_c(C_2)}$.*
- (2) *If we set $C_1 := e \in E^\times$, $C_2 := (eB)\sigma_c(eB) \cdots \sigma_c^{p-2}(eB) \in E^\times$, then $B = \frac{\sigma_a(C_1)}{C_1} \frac{C_2}{\sigma_c(C_2)}$.*

Proof. We have

$$N_{\sigma_a \sigma_c}(B) = \frac{N_{\sigma_a \sigma_c}(\alpha)}{N_{\sigma_a \sigma_c}(\gamma)} = \frac{N_{\sigma_a}(\alpha)}{N_{\sigma_c}(\gamma)} = \frac{b}{b} = 1.$$

Hence by Hilbert's Theorem 90, there exists $e \in E^\times$ such that $B = \frac{\sigma_a \sigma_c(e)}{e}$.

(1) Clearly, we have

$$\frac{\sigma_a(C_1)}{C_1} \frac{C_2}{\sigma_c(C_2)} = \frac{\sigma_a(\sigma_c(e))}{\sigma_c(e)} \frac{e^{-1}}{\sigma_c(e^{-1})} = \frac{\sigma_a \sigma_c(e)}{e} = B.$$

(2) From $B = \frac{\sigma_a \sigma_c(e)}{e}$, we see that $eB = \sigma_a \sigma_c(e)$. Hence $\sigma_c^{p-1}(eB) = \sigma_a(e)$. Therefore

$$B = \frac{\sigma_a(e)}{e} \frac{eB}{\sigma_c^{p-1}(eB)} = \frac{\sigma_a(C_1)}{C_1} \frac{C_2}{\sigma_c(C_2)}. \quad \square$$

Theorem 3.7. *Let the notation and assumption be as in Lemma 3.4. Let $M := E(\sqrt[p]{\delta}, \sqrt[p]{A}, \sqrt[p]{C}, \sqrt[p]{b})$. Then M/F is a Galois extension, M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$, and $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$.*

Proof. Let W^* be the \mathbb{F}_p -vector space in $E^\times / (E^\times)^p$ generated by $[b]_E, [A]_E, [C]_E$ and $[\delta]_E$. Here for any $0 \neq x$ in a field L , we denote $[x]_L$ the image of x in $L^\times / (L^\times)^p$. Since

- (1) $\sigma_c(\delta) = \delta A C_1^{-p}$ (by Lemma 3.4),
- (2) $\sigma_a(\delta) = \delta C C_2^{-p}$ (by Lemma 3.4),
- (3) $\sigma_a(A) = A \frac{b}{a^p}$ (by Lemma 2.1),
- (4) $\sigma_c(C) = C \frac{b}{\gamma^p}$ (by Lemma 2.1),

we see that W^* is in fact an $\mathbb{F}_p[G]$ -module. Hence M/F is a Galois extension by Kummer theory.

Claim: $\dim_{\mathbb{F}_p}(W^*) = 4$. Hence $[L : F] = [L : E][E : F] = p^4 p^2 = p^6$.

Proof of Claim: From our hypothesis that $\dim_{\mathbb{F}_p}\langle [a]_F, [b]_F, [c]_F \rangle = 3$, we see that $\langle [b]_E \rangle \simeq \mathbb{F}_p$.

Clearly, $\langle [b]_E \rangle \subseteq (W^*)^G$. From (3) one gets the relation

$$[\sigma_a(A)]_E = [A]_E [b]_E.$$

This implies that $[A]_E$ is not in $(W^*)^G$. Hence $\dim_{\mathbb{F}_p}\langle [b]_E, [A]_E \rangle = 2$.

From (4) one gets the relation

$$[\sigma_c(C)]_E = [C]_E [b]_E.$$

This implies that $[C]_E$ is not in $(W^*)^{\sigma_c}$. But we have $\langle [b]_E, [A]_E \rangle \subseteq (W^*)^{\sigma_c}$. Hence

$$\dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E \rangle = 3.$$

Observe that the element $(\sigma_a - 1)(\sigma_c - 1)$ annihilates the $\mathbb{F}_p[G]$ -module $\langle [b]_E, [A]_E, [C]_E \rangle$, while by (1) and (3) one has

$$(\sigma_a - 1)(\sigma_c - 1)[\delta]_E = \frac{\sigma_a([A]_E)}{[A]_E} = [b]_E.$$

Therefore one has

$$\dim_{\mathbb{F}_p} W^* = \dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E, [\delta]_E \rangle = 4.$$

Let $H^{a,b} = F(\sqrt[p]{a}, \sqrt[p]{A}, \sqrt[p]{b})$ and $H^{b,c} = F(\sqrt[p]{c}, \sqrt[p]{C}, \sqrt[p]{b})$. Let

$$N := H^{a,b}H^{b,c} = F(\sqrt[p]{a}, \sqrt[p]{c}, \sqrt[p]{b}, \sqrt[p]{A}, \sqrt[p]{C}) = E(\sqrt[p]{b}, \sqrt[p]{A}, \sqrt[p]{C}).$$

Then N/F is a Galois extension of degree p^5 . This is because $\text{Gal}(N/E)$ is dual to the $\mathbb{F}_p[G]$ -submodule $\langle [b]_E, [A]_E, [C]_E \rangle$ via Kummer theory, and the proof of the claim above shows that $\dim_{\mathbb{F}_p} \langle [b]_E, [A]_E, [C]_E \rangle = 3$. We have the following commutative diagram

$$\begin{array}{ccc} \text{Gal}(N/F) & \longrightarrow & \text{Gal}(H^{a,b}/F) \\ \downarrow & & \downarrow \\ \text{Gal}(H^{b,c}/F) & \longrightarrow & \text{Gal}(F(\sqrt[p]{b})/F). \end{array}$$

So we have a homomorphism η from $\text{Gal}(N/F)$ to the pull-back $\text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\sqrt[p]{b})/F)} \text{Gal}(H^{a,b}/F)$:

$$\eta: \text{Gal}(N/F) \longrightarrow \text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\sqrt[p]{b})/F)} \text{Gal}(H^{a,b}/F),$$

which make the obvious diagram commute. We claim that η is injective. Indeed, let σ be an element in $\ker \eta$. Then $\sigma|_{H^{a,b}} = 1$ in $\text{Gal}(H^{a,b}/F)$, and $\sigma|_{H^{b,c}} = 1$ in $\text{Gal}(H^{b,c}/F)$. Since N is the compositum of $H^{a,b}$ and $H^{b,c}$, this implies that $\sigma = 1$, as desired.

Since $|\text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\sqrt[p]{b})/F)} \text{Gal}(H^{a,b}/F)| = p^5 = |\text{Gal}(N/F)|$, we see that η is actually an isomorphism. As in the proof of Proposition 2.2, we can choose an extension $\sigma_a \in \text{Gal}(H^{a,b}/F)$ of $\sigma_a \in \text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b})/F)$ (more precisely, of $\sigma_a|_{F(\sqrt[p]{a}, \sqrt[p]{b})} \in \text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b})/F)$) in such a way that

$$\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha}.$$

Since the square commutative diagram above is a pull-back, we can choose an extension $\sigma_a \in \text{Gal}(N/F)$ of $\sigma_a \in \text{Gal}(H^{a,b}/F)$ in such a way that

$$\sigma_a|_{H^{b,c}} = 1.$$

Now we can choose any extension $\sigma_a \in \text{Gal}(M/F)$ of $\sigma_a \in \text{Gal}(N/F)$. Then we have

$$\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha} \quad \text{and} \quad \sigma_a|_{H^{b,c}} = 1.$$

Similarly, we can choose an extension $\sigma_c \in \text{Gal}(M/F)$ of $\sigma_c \in \text{Gal}(F(\sqrt[p]{b}, \sqrt[p]{c})/F)$ in such a way that

$$\sigma_c(\sqrt[p]{C}) = \sqrt[p]{C} \frac{\sqrt[p]{b}}{\gamma}, \quad \text{and} \quad \sigma_c|_{H^{a,b}} = 1.$$

We define $\sigma_b \in \text{Gal}(M/E)$ to be the element which is dual to $[b]_E$ via Kummer theory. In other words, we require that

$$\sigma_b(\sqrt[p]{b}) = \zeta \sqrt[p]{b},$$

and σ_b acts trivially on $\sqrt[p]{A}$, $\sqrt[p]{C}$ and $\sqrt[p]{\delta}$. We consider σ_b as an element in $\text{Gal}(M/F)$, then it is clear that σ_b is an extension of $\sigma_b \in \text{Gal}(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$. Let $W = \text{Gal}(M/E)$, and let $H = \text{Gal}(M/F)$, then we have the following exact sequence

$$1 \rightarrow W \rightarrow H \rightarrow G \rightarrow 1.$$

By Kummer theory, it follows that W is dual to W^* , and hence $W \simeq (\mathbb{Z}/p\mathbb{Z})^4$. In particular, we have $|H| = p^6$.

Recall that from [BD, Theorem 1], we know that the group $\mathbb{U}_4(\mathbb{F}_p)$ has a presentation with generators s_1, s_2, s_3 subject to the following relations

$$\begin{aligned} (R) \quad & s_1^p = s_2^p = s_3^p = 1, \\ & [s_1, s_3] = 1, \\ & [s_1, [s_1, s_2]] = [s_2, [s_1, s_2]] = 1, \\ & [s_2, [s_2, s_3]] = [s_3, [s_2, s_3]] = 1, \\ & [[s_1, s_2], [s_2, s_3]] = 1. \end{aligned}$$

Note that $|\text{Gal}(M/F)| = p^6$. So in order to show that $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$, we shall show that σ_a, σ_b and σ_c generate $\text{Gal}(M/F)$ and that they satisfy these above relations.

Claim: The elements σ_a, σ_b and σ_c generate $\text{Gal}(M/F)$.

Proof of Claim: Let K be the maximal p -elementary subextension of M . Note that $\text{Gal}(M/F)$ is a p -group. So in order to show that σ_a, σ_b and σ_c generate $\text{Gal}(M/F)$, we only need to show that (the restrictions of) these elements generate $\text{Gal}(K/F)$ by the Burnside basis theorem. (See e.g. [Ha, Theorem 12.2.1] or [Ko, Theorem 4.10].) We shall now determine the field K . By Kummer theory, $K = F(\sqrt[p]{\Delta})$, where $\Delta = (F^\times \cap M^{\times p})/(F^\times)^p$. Let $[f]_F$ be any element in Δ , where $f \in F^\times \cap (M^\times)^p \subseteq E^\times \cap (M^\times)^p$. By Kummer theory, one has $W^* = (E^\times \cap (M^\times)^p)/(E^\times)^p$. Hence we can write

$$[f]_E = [\delta]_E^{\epsilon_\delta} [A]_E^{\epsilon_A} [C]_E^{\epsilon_C} [b]_E^{\epsilon_b},$$

where $\epsilon_\delta, \epsilon_A, \epsilon_C, \epsilon_b \in \mathbb{Z}$. By applying $(\sigma_a - 1)(\sigma_c - 1)$ on $[f]_E$ we get $[1]_E = [b]_E^{\epsilon_\delta}$. (See the proof of the first claim of this proof.) Thus ϵ_δ is divisible by p , and one has

$$[f]_E = [A]_E^{\epsilon_A} [C]_E^{\epsilon_C} [b]_E^{\epsilon_b}.$$

By applying $\sigma_a - 1$ on both sides of this equation, we get $[1]_E = [b]_E^{\epsilon_A}$. Thus ϵ_A is divisible by p . Similarly, ϵ_C is also divisible by p . Hence $f = b^{\epsilon_b} e^p$ for some $e \in E$. Since b and f are in F , e^p is in $F^\times \cap (E^\times)^p$ and $[e^p]_F$ is in $\langle [a]_F, [c]_F \rangle$. Therefore $[f]_F$ is in $\langle [a]_F, [b]_F, [c]_F \rangle$ and

$$\Delta = \langle [a]_F, [b]_F, [c]_F \rangle.$$

So $K = F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$. Then it is clear that σ_a, σ_b and σ_c generate $\text{Gal}(K/F)$ and the claim follows.

Claim: The order of σ_a is p .

Proof of Claim: As in the proof of Proposition 2.2, we see that $\sigma_a^p(\sqrt[p]{A}) = \sqrt[p]{A}$.

Since $\sigma_a(\delta) = \delta C C_2^{-p}$ (equation (2)), one has $\sigma_a(\sqrt[p]{\delta}) = \xi^i \sqrt[p]{\delta} \sqrt[p]{C} C_2^{-1}$ for some $i \in \mathbb{Z}$. This implies that

$$\begin{aligned} \sigma_a^2(\sqrt[p]{\delta}) &= \xi^i \sigma_a(\sqrt[p]{\delta}) \sigma_a(\sqrt[p]{C}) \sigma_a(C_2)^{-1} \\ &= \xi^{2i} \sqrt[p]{\delta} (\sqrt[p]{C})^2 C_2^{-1} \sigma_a(C_2)^{-1}. \end{aligned}$$

Inductively, we obtain

$$\begin{aligned} \sigma_a^p(\sqrt[p]{\delta}) &= \xi^{pi} \sqrt[p]{\delta} (\sqrt[p]{C})^p N_{\sigma_a}(C_2)^{-1} \\ &= \sqrt[p]{\delta} (C) N_{\sigma_a}(C_2)^{-1} \\ &= \sqrt[p]{\delta}. \end{aligned}$$

Therefore, we can conclude that $\sigma_a^p = 1$, and σ_a is of order p .

Claim: The order of σ_b is p .

Proof of Claim: This is clear because σ_b acts trivially on $\sqrt[p]{A}, \sqrt[p]{C}, \delta, E$ and $\sigma_b(\sqrt[p]{b}) = \xi \sqrt[p]{b}$.

Claim: The order of σ_c is p .

Proof of Claim: As in the proof of Proposition 2.2, we see that $\sigma_c^p(\sqrt[p]{C}) = \sqrt[p]{C}$.

Since $\sigma_c(\delta) = \delta A C_1^{-p}$ (equation (1)), one has $\sigma_c(\sqrt[p]{\delta}) = \xi^j \sqrt[p]{\delta} \sqrt[p]{A} C_1^{-1}$ for some $j \in \mathbb{Z}$. This implies that

$$\begin{aligned} \sigma_c^2(\sqrt[p]{\delta}) &= \xi^j \sigma_c(\sqrt[p]{\delta}) \sigma_c(\sqrt[p]{A}) \sigma_c(C_1)^{-1} \\ &= \xi^{2j} \sqrt[p]{\delta} (\sqrt[p]{A})^2 C_1^{-1} \sigma_c(C_1)^{-1}. \end{aligned}$$

Inductively, we obtain

$$\begin{aligned} \sigma_c^p(\sqrt[p]{\delta}) &= \xi^{pj} \sqrt[p]{\delta} (\sqrt[p]{A})^p N_{\sigma_c}(C_1)^{-1} \\ &= \sqrt[p]{\delta} (A) N_{\sigma_c}(C_1)^{-1} \\ &= \sqrt[p]{\delta}. \end{aligned}$$

Therefore, we can conclude that $\sigma_c^p = 1$, and σ_c is of order p .

Claim: $[\sigma_a, \sigma_c] = 1$.

Proof of Claim: It is enough to check that $\sigma_a \sigma_c(\sqrt[p]{\delta}) = \sigma_c \sigma_a(\sqrt[p]{\delta})$.

We have

$$\begin{aligned}
\sigma_a \sigma_c(\sqrt[p]{\delta}) &= \sigma_a(\xi^j \sqrt[p]{\delta} \sqrt[p]{A} C_1^{-1}) \\
&= \xi^j \sigma_a(\sqrt[p]{\delta}) \sigma_a(\sqrt[p]{A}) \sigma_a(C_1)^{-1} \\
&= \xi^j \xi^i \sqrt[p]{\delta} \sqrt[p]{C} C_2^{-1} \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha} \sigma_a(C_1)^{-1} \\
&= \xi^{i+j} \sqrt[p]{\delta} \sqrt[p]{C} \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha} (\sigma_a(C_1) C_2)^{-1} \\
&= \xi^{i+j} \sqrt[p]{\delta} \sqrt[p]{C} \sqrt[p]{A} \frac{\sqrt[p]{b}}{\alpha} \frac{(C_1 \sigma_c(C_2))^{-1}}{B} \\
&= \xi^{i+j} \sqrt[p]{\delta} \sqrt[p]{C} \sqrt[p]{A} \frac{\sqrt[p]{b}}{\gamma} (C_1 \sigma_c(C_2))^{-1}.
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
\sigma_c \sigma_a(\sqrt[p]{\delta}) &= \sigma_c(\xi^i \sqrt[p]{\delta} \sqrt[p]{C} C_2^{-1}) \\
&= \xi^i \sigma_c(\sqrt[p]{\delta}) \sigma_c(\sqrt[p]{C}) \sigma_c(C_2)^{-1} \\
&= \xi^i \xi^j \sqrt[p]{\delta} \sqrt[p]{A} C_1^{-1} \sqrt[p]{C} \frac{\sqrt[p]{b}}{\gamma} \sigma_c(C_2)^{-1} \\
&= \xi^{i+j} \sqrt[p]{\delta} \sqrt[p]{A} \sqrt[p]{C} \frac{\sqrt[p]{b}}{\gamma} (C_1 \sigma_c(C_2))^{-1}.
\end{aligned}$$

Therefore, $\sigma_a \sigma_c(\sqrt[p]{\delta}) = \sigma_c \sigma_a(\sqrt[p]{\delta})$, as desired.

Claim: $[\sigma_a, [\sigma_a, \sigma_b]] = [\sigma_b, [\sigma_a, \sigma_b]] = 1$.

Proof of Claim: Since G is abelian, it follows that $[\sigma_a, \sigma_b]$ is in W . Now both σ_b and $[\sigma_a, \sigma_b]$ are in W . Hence $[\sigma_b, [\sigma_a, \sigma_b]] = 1$ because W is abelian.

Now we show that $[\sigma_a, [\sigma_a, \sigma_b]] = 1$. Since the Heisenberg group $\mathbb{U}_3(\mathbb{F}_p)$ is a nilpotent group of nilpotent length 2, we see that $[\sigma_a, [\sigma_a, \sigma_b]] = 1$ on $H^{a,b}$ and $H^{b,c}$. So it is enough to check that $[\sigma_a, [\sigma_a, \sigma_b]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

From the choice of σ_b , we see that

$$\sigma_b \sigma_a(\sqrt[p]{\delta}) = \sigma_a(\sqrt[p]{\delta}) = \sigma_a \sigma_b(\sqrt[p]{\delta}).$$

Hence, $[\sigma_a, \sigma_b](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$. Since σ_a and σ_b act trivially on $\sqrt[p]{C}$, and σ_b acts trivially on E , we see that

$$[\sigma_a, \sigma_b](\sqrt[p]{C}) = \sqrt[p]{C}, \quad \text{and} \quad [\sigma_a, \sigma_b](C_2^{-1}) = C_2^{-1}.$$

We have

$$\begin{aligned}
[\sigma_a, \sigma_b] \sigma_a(\sqrt[p]{\delta}) &= [\sigma_a, \sigma_b](\xi^i \sqrt[p]{\delta} \sqrt[p]{C} C_2^{-1}) \\
&= [\sigma_a, \sigma_b](\xi^i) [\sigma_a, \sigma_b](\sqrt[p]{\delta}) [\sigma_a, \sigma_b](\sqrt[p]{C}) [\sigma_a, \sigma_b](C_2^{-1}) \\
&= \xi^i \sqrt[p]{\delta} \sqrt[p]{C} C_2^{-1} \\
&= \sigma_a(\sqrt[p]{\delta}) \\
&= \sigma_a[\sigma_a, \sigma_b](\sqrt[p]{\delta}).
\end{aligned}$$

Thus $[\sigma_a, [\sigma_a, \sigma_b]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$, as desired.

Claim: $[\sigma_b, [\sigma_b, \sigma_c]] = [\sigma_c, [\sigma_b, \sigma_c]] = 1$.

Proof of Claim: Since G is abelian, it follows that $[\sigma_b, \sigma_c]$ is in W . Now both σ_b and $[\sigma_b, \sigma_c]$ are in W . Hence $[\sigma_b, [\sigma_b, \sigma_c]] = 1$ because W is abelian.

Now we show that $[\sigma_c, [\sigma_b, \sigma_c]] = 1$. Since the Heisenberg group $\mathbb{U}_3(\mathbb{F}_p)$ is a nilpotent group of nilpotent length 2, we see that $[\sigma_c, [\sigma_b, \sigma_c]] = 1$ on $H^{a,b}$ and $H^{b,c}$. So it is enough to check that $[\sigma_c, [\sigma_b, \sigma_c]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

From the choice of σ_b , we see that

$$\sigma_b \sigma_c(\sqrt[p]{\delta}) = \sigma_c(\sqrt[p]{\delta}) = \sigma_c \sigma_b(\sqrt[p]{\delta}).$$

Hence, $[\sigma_b, \sigma_c](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$. Since σ_b and σ_c act trivially on $\sqrt[p]{A}$, and σ_b acts trivially on E , we see that

$$[\sigma_b, \sigma_c](\sqrt[p]{A}) = \sqrt[p]{A}, \quad \text{and} \quad [\sigma_b, \sigma_c](C_1^{-1}) = C_1^{-1}.$$

We have

$$\begin{aligned}
[\sigma_b, \sigma_c] \sigma_c(\sqrt[p]{\delta}) &= [\sigma_b, \sigma_c](\xi^j \sqrt[p]{\delta} \sqrt[p]{A} C_1^{-1}) \\
&= [\sigma_b, \sigma_c](\xi^j) [\sigma_b, \sigma_c](\sqrt[p]{\delta}) [\sigma_b, \sigma_c](\sqrt[p]{A}) [\sigma_b, \sigma_c](C_1^{-1}) \\
&= \xi^j \sqrt[p]{\delta} \sqrt[p]{A} C_1^{-1} \\
&= \sigma_c(\sqrt[p]{\delta}) \\
&= \sigma_c[\sigma_a, \sigma_b](\sqrt[p]{\delta}).
\end{aligned}$$

Thus $[\sigma_c, [\sigma_b, \sigma_c]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$, as desired.

Claim: $[[\sigma_a, \sigma_b], [\sigma_b, \sigma_c]] = 1$.

Proof of Claim: Since G is abelian, $[\sigma_a, \sigma_b]$ and $[\sigma_b, \sigma_c]$ are in W . Hence $[[\sigma_a, \sigma_b], [\sigma_b, \sigma_c]] = 1$ because W is abelian.

An explicit isomorphism $\varphi: \text{Gal}(M/F) \rightarrow \mathbb{U}_4(\mathbb{F}_p)$ may be defined as

$$\sigma_a \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_c \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

□

Example 3.8. Let the notation and assumption be as in Lemma 3.4. Let us consider the case $p = 2$. In Lemma 3.6, we can choose $e = \frac{\alpha}{\alpha + \gamma}$. (Observe that $\alpha + \gamma \neq 0$.) In fact, one can easily check that

$$\sigma_a \sigma_c \left(\frac{\alpha}{\alpha + \gamma} \right) = \frac{\gamma}{\alpha} \frac{\alpha}{\alpha + \gamma}.$$

(1) If we choose $C_1 = \sigma_c(e)$ and $C_2 = e^{-1}$ as in Lemma 3.6 part (1), then we have

$$\begin{aligned} A &= N_{\sigma_c}(C_1) = N_{\sigma_c}(e) = \frac{\alpha^2 \gamma}{(\alpha + \gamma)(\alpha \gamma + b)}, \\ C &= N_{\sigma_a}(C_2) = N_{\sigma_a}(e^{-1}) = \frac{(\alpha + \gamma)(\alpha \gamma + b)}{b \alpha}. \end{aligned}$$

In Lemma 3.4, we can choose $\delta = e^{-1} = \frac{\alpha + \gamma}{\alpha}$. In fact, we have

$$\begin{aligned} \frac{\sigma_c(\delta)}{\delta} &= \sigma_c(e)^{-1} e = \sigma_c(e)^{-2} e \sigma_c(e) = C_1^{-2} N_{\sigma_c}(e) = A C_1^{-2}, \\ \frac{\sigma_a(\delta)}{\delta} &= \sigma_a(e^{-1}) e = e^{-1} \sigma_a(e^{-1}) e^2 = N_{\sigma_a}(e^{-1}) C_2^{-2} = C C_2^{-2}. \end{aligned}$$

Therefore

$$\begin{aligned} M &= F(\sqrt{b}, \sqrt{A}, \sqrt{C}, \sqrt{\delta}) = F\left(\sqrt{b}, \sqrt{\frac{\alpha^2 \gamma}{(\alpha + \gamma)(\alpha \gamma + b)}}, \sqrt{\frac{(\alpha + \gamma)(\alpha \gamma + b)}{b \alpha}}, \sqrt{\frac{\alpha + \gamma}{\alpha}}\right) \\ &= F\left(\sqrt{b}, \sqrt{\frac{\alpha + \gamma}{\alpha}}, \sqrt{\alpha \gamma + b}, \sqrt{\alpha \gamma}\right). \end{aligned}$$

(2) If we choose $C_1 = e = \frac{\alpha}{\alpha + \gamma}$ and $C_2 = eB = \frac{\gamma}{\alpha + \gamma}$ as in Lemma 3.6 part (2), then we have

$$\begin{aligned} A &= N_{\sigma_c}(C_1) = N_{\sigma_c}(e) = \frac{\alpha^2 \gamma}{(\alpha + \gamma)(\alpha \gamma + b)}, \\ C &= N_{\sigma_a}(C_2) = N_{\sigma_a}(eB) = \frac{\gamma^2 \alpha}{(\alpha + \gamma)(\alpha \gamma + b)}. \end{aligned}$$

In Lemma 3.4, we can choose $\delta = (\alpha + \gamma)^{-1}$. In fact, we have

$$\begin{aligned} \frac{\sigma_c(\delta)}{\delta} &= \frac{\gamma(\alpha + \gamma)}{\alpha \gamma + b} = A C_1^{-2}, \\ \frac{\sigma_a(\delta)}{\delta} &= \frac{\alpha(\alpha + \gamma)}{\alpha \gamma + b} = C C_2^{-2}. \end{aligned}$$

Therefore

$$M = F(\sqrt{b}, \sqrt{A}, \sqrt{C}, \sqrt{\delta}) = F(\sqrt{b}, \sqrt{\frac{\alpha^2\gamma}{\alpha\gamma+b'}}, \sqrt{\frac{\alpha\gamma^2}{\alpha\gamma+b'}}, \sqrt{\alpha+\gamma}).$$

Observe also that M is the Galois closure of $E(\sqrt{\delta}) = F(\sqrt{a}, \sqrt{c}, \sqrt{\alpha+\gamma})$.

3.2. Fields of characteristic not p . Let F_0 be an arbitrary field of characteristic $\neq p$. We fix a primitive p -th root of unity ξ , and let $F = F_0(\xi)$. Then F/F_0 is a cyclic extension of degree $d = [F : F_0]$. Observe that d divides $p-1$. We choose an integer ℓ such that $d\ell \equiv 1 \pmod{p}$. Let σ_0 be a generator of $H := \text{Gal}(F/F_0)$. Then $\sigma_0(\xi) = \xi^e$ for an $e \in \mathbb{Z} \setminus p\mathbb{Z}$.

Let χ_1, χ_2, χ_3 be elements in $\text{Hom}(G_{F_0}, \mathbb{F}_p) = H^1(G_{F_0}, \mathbb{F}_p)$. We assume that χ_1, χ_2, χ_3 are \mathbb{F}_p -linearly independent and $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$. By [MT4, Lemma 2.6], the homomorphism $(\chi_1, \chi_2, \chi_3): G_{F_0} \rightarrow (\mathbb{F}_p)^3$ is surjective. Let L_0 be the fixed field of $(F_0)^s$ under the kernel of the surjection $(\chi_1, \chi_2, \chi_3): G_{F_0} \rightarrow (\mathbb{F}_p)^3$. Then L_0/F_0 is Galois with $\text{Gal}(L_0/F_0) \simeq (\mathbb{F}_p)^3$. We shall construct a Galois extension M_0/F_0 such that $\text{Gal}(M_0/F_0) \simeq \mathbb{U}_4(\mathbb{F}_p)$ and M_0 contains L_0 .

The restrictions $\text{res}_{G_F}(\chi_1), \text{res}_{G_F}(\chi_2), \text{res}_{G_F}(\chi_3)$ are elements in $\text{Hom}(G_F, \mathbb{F}_p)$. They are \mathbb{F}_p -linearly independent and $\text{res}_{G_F}(\chi_1) \cup \text{res}_{G_F}(\chi_2) = \text{res}_{G_F}(\chi_2) \cup \text{res}_{G_F}(\chi_3) = 0$. By Kummer theory there exist a, b, c in F^\times such that $\text{res}_{G_F}(\chi_1) = \chi_a, \text{res}_{G_F}(\chi_2) = \chi_b, \text{res}_{G_F}(\chi_3) = \chi_c$. Then we have $(a, b) = (b, c) = 0$ in $H^2(G_F, \mathbb{F}_p)$.

Let $L = L_0(\xi)$. Then $L = F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$, and L/F is Galois with $\text{Gal}(L/F) \simeq \text{Gal}(L_0/F_0) \simeq (\mathbb{F}_p)^3$.

Claim 1: L/F_0 is Galois with $\text{Gal}(L/F_0) \simeq \text{Gal}(F/F_0) \times \text{Gal}(L/F)$.

Proof of Claim: Since L_0/F_0 and F/F_0 are Galois extensions of relatively prime degrees, the claim follows.

We define $\Phi := \ell \left[\sum_{i=0}^{d-1} e^i \sigma_0^{-i} \right] \in \mathbb{Z}[H]$. The group ring $\mathbb{Z}[H]$ acts on F in the obvious way, and if we let H act trivially on L_0 we get an action on L also. Then Φ determines a map

$$\Phi: L \rightarrow L, x \mapsto \Phi(x).$$

For convenience, we shall denote $\tilde{x} := \Phi(x)$.

The claim above implies that $\Phi\sigma = \sigma\Phi$ for every $\sigma \in \text{Gal}(L/F)$.

Claim 2: We have $\tilde{a} = a$ modulo $(F^\times)^p$; $\tilde{b} = b$ modulo $(F^\times)^p$, $\tilde{c} = c$ modulo $(F^\times)^p$.

Proof of Claim: A similar argument as in the proof of Claim 1 shows that $F(\sqrt[p]{a})/F_0$ is Galois with $\text{Gal}(F(\sqrt[p]{a})/F_0) = \text{Gal}(F(\sqrt[p]{a})/F) \times \text{Gal}(F/F_0)$. Since both groups $\text{Gal}(F(\sqrt[p]{a})/F)$ and $\text{Gal}(F/F_0)$ are cyclic and of coprime orders, we see that the extension $F(\sqrt[p]{a})/F_0$ is cyclic. By Albert's result (see [Alb, pages 209-211] and [Wat, Section 5]), we have

$\sigma_0 a = a^e$ modulo $(F^\times)^p$. Hence for all integers i , $\sigma_0^i(a) = a^{e^i} \bmod (F^\times)^p$. Thus $\sigma_0^{-i}(a^{e^i}) = a \bmod (F^\times)^p$. Therefore, we have

$$\tilde{a} = \Phi(a) = \left[\prod_{i=0}^{d-1} \sigma_0^{-i}(a^{e^i}) \right]^\ell = \left[\prod_{i=0}^{d-1} a \right]^\ell = a^{d\ell} = a \bmod (F^\times)^p.$$

Similarly, we have $\tilde{b} = b$ modulo $(F^\times)^p$, $\tilde{c} = c$ modulo $(F^\times)^p$.

Claim 3: For every $x \in L$, we have $\frac{\sigma_0 \tilde{x}}{\tilde{x}^e} = \sigma_0(x^{\ell(1-e^d)/p})^p \in L^p$.

Proof of Claim: This follows from the following identity in the group ring $\mathbb{Z}[H]$,

$$(\sigma_0 - e) \left(\sum_{i=0}^{d-1} e^i \sigma_0^{-i} \right) = \sigma_0(1 - e^d) \equiv 0 \bmod p.$$

By our construction of Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions over fields containing a primitive p -th root of unity (see Subsection 3.1), we have $\alpha, \gamma, B, \dots, A, C, \delta$ such that if we let $M := L(\sqrt[p]{A}, \sqrt[p]{C}, \sqrt[p]{\delta})$, then M/F is a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension. We set $\tilde{M} := L(\sqrt[p]{\tilde{A}}, \sqrt[p]{\tilde{C}}, \sqrt[p]{\tilde{\delta}})$.

Claim 4: \tilde{M}/F is Galois with $\text{Gal}(\tilde{M}/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$.

Proof of Claim: Since Φ commutes with every $\sigma \in \text{Gal}(L/F)$, this implies that \tilde{M}/F is Galois. This, together with Claim 2, also implies that $\text{Gal}(\tilde{M}/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$ because the construction of \tilde{M} over F is obtained in the same way as in the construction of M , except that we replace the data $\{a, b, c, \alpha, \gamma, B, \dots\}$ by their "tilde" counterparts $\{\tilde{a}, \tilde{b}, \tilde{c}, \tilde{\alpha}, \tilde{\gamma}, \tilde{B}, \dots\}$.

Claim 5: \tilde{M}/F_0 is Galois with $\text{Gal}(\tilde{M}/F_0) \simeq \text{Gal}(\tilde{M}/F) \times \text{Gal}(F/F_0)$.

Proof of Claim: By Claim 3, we see that $\sigma_0 \tilde{x} = \tilde{x}^e$ modulo $(L^\times)^p$ for every \tilde{x} in the \mathbb{F}_p -vector subspace \tilde{W}^* of $L^\times / (L^\times)^p$ generated by \tilde{A}, \tilde{C} , and $\tilde{\delta}$. Hence \tilde{W}^* is an $\mathbb{F}_p[\text{Gal}(L/F_0)]$ -module. Therefore \tilde{M}/F_0 is Galois by Kummer theory.

We also have the following exact sequence of groups

$$1 \rightarrow \text{Gal}(\tilde{M}/F) \rightarrow \text{Gal}(\tilde{M}/F_0) \rightarrow \text{Gal}(F/F_0) \rightarrow 1.$$

Since $|\text{Gal}(\tilde{M}/F)|$ and $|\text{Gal}(F/F_0)|$ are coprime, the above sequence is split by Schur-Zassenhaus's theorem. (See [Za, IV.7, Theorem 25].) The Galois group $\text{Gal}(\tilde{M}/F_0)$ is the semidirect product of $\text{Gal}(\tilde{M}/F)$ and $H = \text{Gal}(F/F_0)$, with H acting on $\text{Gal}(\tilde{M}/F)$ by conjugation. We need to show that this product is in fact direct, i.e., that the action of H on $\text{Gal}(\tilde{M}/F)$ is trivial. Note that H has an order coprime to p , and H acts trivially on $\text{Gal}(L/F)$ (see Claim 1) which is the quotient of $\text{Gal}(\tilde{M}/F)$ by its Frattini subgroup. Then a result of P. Hall (see [Ha, Theorem 12.2.2]) implies that H acts trivially on $\text{Gal}(\tilde{M}/F)$.

From the discussion above we obtain the following result.

Theorem 3.9. *Let the notation be as above. Let M_0 be the fixed field of \tilde{M} under the subgroup of $\text{Gal}(\tilde{M}/F_0)$ which is isomorphic to $\text{Gal}(F/F_0)$. Then M_0/F_0 is Galois with $\text{Gal}(M_0/F_0) \simeq \text{Gal}(\tilde{M}/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$, and M_0 contains L_0 .*

Proof. Claim 5 above implies that M_0/F_0 is Galois with $\text{Gal}(M_0/F_0) \simeq \text{Gal}(\tilde{M}/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. Since $H \simeq \text{Gal}(\tilde{M}/M_0)$ acts trivially on L_0 , we see that M_0 contains L_0 .

Let $\sigma_1 := \sigma_a|_{M_0}$, $\sigma_2 := \sigma_b|_{M_0}$ and $\sigma_3 := \sigma_c|_{M_0}$. Then σ_1, σ_2 and σ_3 generate $\text{Gal}(M_0/F_0) \simeq \mathbb{U}_4(\mathbb{F}_p)$. We also have

$$\begin{aligned}\chi_1(\sigma_1) &= 1, \chi_1(\sigma_2) = 0, \chi_1(\sigma_3) = 0; \\ \chi_2(\sigma_1) &= 0, \chi_2(\sigma_2) = 1, \chi_2(\sigma_3) = 0; \\ \chi_3(\sigma_1) &= 0, \chi_3(\sigma_2) = 0, \chi_3(\sigma_3) = 1.\end{aligned}$$

(Note that for each $i = 1, 2, 3$, χ_i is trivial on $\text{Gal}(M/M_0)$, hence $\chi_i(\sigma_j)$ makes sense for every $j = 1, 2, 3$.) An explicit isomorphism $\varphi: \text{Gal}(M_0/F_0) \rightarrow \mathbb{U}_4(\mathbb{F}_p)$ may be defined as

$$\sigma_1 \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_2 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

□

4. THE CONSTRUCTION OF $\mathbb{U}_4(\mathbb{F}_p)$ -EXTENSIONS: THE CASE OF CHARACTERISTIC p

In this section we assume that F is of characteristic $p > 0$. Although by a theorem of Witt (see [Wi] and [Ko, Chapter 9, Section 9.1]), we know that the Galois group of the maximal p -extension of F is a free pro- p -group, finding specific constructions of Galois p -extensions over F can still be challenging. The following construction of an explicit Galois extension M/F with Galois group $\mathbb{U}_4(\mathbb{F}_p)$ is an analogue of the construction in Subsection 3.1 when we assumed that a p -th root of unity is in F . However we find the details interesting, and therefore for the convenience of the reader, we are including them here. Observe that even the case of the explicit construction of Heisenberg extensions of degree p^3 in characteristic p is of interest. In the case when F has characteristic not p , the constructions of Heisenberg extensions of degree p^3 are now classical, important tools in Galois theory. We did not find any such constructions in the literature in the case of characteristic p . Nevertheless the construction in Subsection 4.2 seems to be simple, useful and aesthetically pleasing. What is even more surprising is that the field construction of Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions over a field F of characteristic p in Subsection 4.3 is almost equally simple. We have to check more details to confirm the validity of this construction, but the construction of the required Galois extension M itself, is remarkably simple. The possibility of choosing generators in such a straightforward manner (as described in Theorem 4.3) is striking. It is interesting that the main construction in Section 3 carries over with necessary modifications in the case of characteristic p .

4.1. A brief review of Artin-Schreier theory. (For more details and the origin of this beautiful theory, see [ASch].) Let F be a field of characteristic $p > 0$. Let $\wp(X) = X^p - X$ be the Artin-Schreier polynomial. For each a in F of characteristic p , we let θ_a be a root of $\wp(X) = a$. We also denote $[a]_F$ to be the image of a in $F/\wp(F)$. For each subgroup U of $F/\wp(F)$, let $F_U := F(\theta_u : [u]_F \in U)$. Then the map $U \mapsto F_U$ is a bijection between subgroups of $F/\wp(F)$ and abelian extensions of F of exponent dividing p . There is a pairing

$$\text{Gal}(F_U/F) \times U \rightarrow \mathbb{F}_p,$$

defined by $\langle \sigma, a \rangle = \sigma(\theta_a) - \theta_a$, which is independent of the choice of root θ_a . Artin-Schreier theory says that this pairing is non-degenerate.

Now assume that F/k is a finite Galois extension. The Galois group $\text{Gal}(F/k)$ acts naturally on $F/\wp(F)$. As an easy exercise, one can show that such an extension F_U , where U is a subgroup of $F/\wp(F)$, is Galois over k if and only if U is actually an $\mathbb{F}_p[\text{Gal}(F/k)]$ -module.

4.2. Heisenberg extensions in characteristic $p > 0$. For each $a \in F$, let $\chi_a \in \text{Hom}(G_F, \mathbb{F}_p)$ be the corresponding element associated with a via Artin-Schreier theory. Explicitly, χ_a is defined by

$$\chi_a(\sigma) = \sigma(\theta_a) - \theta_a.$$

Assume that a, b are elements in F , which are linearly independent modulo $\wp(F)$. Let $K = F(\theta_a, \theta_b)$. Then K/F is a Galois extension whose Galois group is generated by σ_a and σ_b . Here $\sigma_a(\theta_b) = \theta_b$, $\sigma_a(\theta_a) = \theta_a + 1$; $\sigma_b(\theta_a) = \theta_a$, $\sigma_b(\theta_b) = \theta_b + 1$.

We set $A = b\theta_a$. Then

$$\sigma_a(A) = A + b, \text{ and } \sigma_b(A) = A.$$

Proposition 4.1. *Let the notation be as above. Let $L = K(\theta_A)$. Then L/F is Galois whose Galois group is isomorphic to $\mathbb{U}_3(\mathbb{F}_p)$.*

Proof. From $\sigma_a(A) - A = b \in \wp(K)$, and $\sigma_b(A) = A$, we see that $\sigma(A) - A \in \wp(K)$ for every $\sigma \in \text{Gal}(K/F)$. This implies that the extension $L := K(\theta_A)/F$ is Galois. Let $\tilde{\sigma}_a \in \text{Gal}(L/F)$ (resp. $\tilde{\sigma}_b \in \text{Gal}(L/F)$) be an extension of σ_a (resp. σ_b). Since $\sigma_b(A) = A$, we have $\tilde{\sigma}_b(\theta_A) = \theta_A + j$, for some $j \in \mathbb{F}_p$. Hence $\tilde{\sigma}_b^p(\theta_A) = \theta_A$. This implies that $\tilde{\sigma}_b$ is of order p .

On the other hand, we have

$$\wp(\tilde{\sigma}_a(\theta_A)) = \sigma_a(A) = A + b.$$

Hence $\tilde{\sigma}_a(\theta_A) = \theta_A + \theta_b + i$, for some $i \in \mathbb{F}_p$. Then

$$\tilde{\sigma}_a^p(\theta_A) = \theta_A + p\theta_b + pi = \theta_A.$$

This implies that $\tilde{\sigma}_a$ is also of order p . We have

$$\tilde{\sigma}_a \tilde{\sigma}_b(\theta_A) = \tilde{\sigma}_a(j + \theta_A) = i + j + \theta_A + \theta_b,$$

$$\tilde{\sigma}_b \tilde{\sigma}_a(\theta_A) = \tilde{\sigma}_b(i + \theta_A + \theta_b) = i + j + \theta_A + 1 + \theta_b.$$

We set $\tilde{\sigma}_A := \tilde{\sigma}_a \tilde{\sigma}_b \tilde{\sigma}_a^{-1} \tilde{\sigma}_b^{-1}$. Then

$$\tilde{\sigma}_A(\theta_A) = \theta_A - 1.$$

This implies that $\tilde{\sigma}_A$ is of order p and that $\text{Gal}(L/F)$ is generated by $\tilde{\sigma}_a$ and $\tilde{\sigma}_b$. We also have

$$\tilde{\sigma}_a \tilde{\sigma}_A = \tilde{\sigma}_A \tilde{\sigma}_a, \text{ and } \tilde{\sigma}_b \tilde{\sigma}_A = \tilde{\sigma}_A \tilde{\sigma}_b.$$

We can define an isomorphism $\varphi: \text{Gal}(L/F) \rightarrow \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ by letting

$$\tilde{\sigma}_a \mapsto \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tilde{\sigma}_b \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \tilde{\sigma}_A \mapsto \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note that $[L : F] = p^3$. Hence there are exactly p extensions of $\sigma_a \in \text{Gal}(K/F)$ to the automorphisms in $\text{Gal}(L/F)$ since $[L : K] = p^3/p^2 = p$. Therefore for later use, we can choose an extension of $\sigma_a \in \text{Gal}(K/F)$, which we shall denote $\sigma_a \in \text{Gal}(L/F)$ with a slight abuse of notation, in such a way that $\sigma_a(\theta_A) = \theta_A + \theta_b$. \square

Remark 4.2. It is interesting to compare our choices of generators A of Heisenberg extensions over given bicyclic extensions in the case of characteristic p and the case when the base field in fact contains a primitive p -th root of unity. See the proofs of Proposition 2.2 and the proposition above. Although the form of A in Proposition 2.2 is more complicated than the strikingly simple choice above, the basic principle for the search of a suitable A is the same in both cases. We need to guarantee that $\sigma_a(A)/A \in (K^\times)^p$ and $\sigma_a(A) - A \in \wp(K)$ in order that $K(\sqrt[p]{A})$ and $K(\theta_A)$ are Galois over F . Further, in order to guarantee that σ_a and σ_b will not commute, we want $\sigma_a(A)/A = bk^p$, for some $k \in K^\times$, where σ_b acts trivially on k . Similarly in the characteristic p case we want $\sigma_a(A) - A = b + \wp(k)$, where $\sigma_b(k) = k$. If $\text{char}(F) = p$, then this is always possible in a simple way above with k even being 0. (See also [JLY, Appendix A.1, Example], where the authors discuss a construction of quaternion Q_8 -extensions over fields of characteristic 2.) In the case when F contains a primitive p -th root of unity, the search for a suitable A leads to the norm condition $N_{F(\sqrt[p]{a})/F}(\alpha) = b$. For some related considerations see [MS1, Section 2].

4.3. Construction of Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions. We assume that we are given elements a, b and c in F such that a, b and c are linearly independent modulo $\wp(F)$. We shall construct a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension M/F such that M contains $F(\theta_a, \theta_b, \theta_c)$.

First we note that $F(\theta_a, \theta_b, \theta_c)/F$ is a Galois extension with $\text{Gal}(F(\theta_a, \theta_b, \theta_c)/F)$ generated by $\sigma_a, \sigma_b, \sigma_c$. Here

$$\begin{aligned} \sigma_a(\theta_a) &= 1 + \theta_a, \sigma_a(\theta_b) = \theta_b, \sigma_a(\theta_c) = \theta_c; \\ \sigma_b(\theta_a) &= \theta_a, \sigma_b(\theta_b) = 1 + \theta_b, \sigma_b(\theta_c) = \theta_c; \\ \sigma_c(\theta_a) &= \theta_a, \sigma_c(\theta_b) = \theta_b, \sigma_c(\theta_c) = 1 + \theta_c. \end{aligned}$$

Recall that $A = b\theta_a$. We set $C := b\theta_c$. We set $\delta := (AC)/b = b\theta_a\theta_c \in E := F(\theta_a, \theta_c)$. Then we have

$$\begin{aligned}\sigma_a(\delta) - \delta &= b\sigma_a(\theta_a)\sigma_a(\theta_c) - b\theta_a\theta_c = b[\sigma_a(\theta_a) - \theta_a]\theta_c = b\theta_c = C, \\ \sigma_c(\delta) - \delta &= b\sigma_c(\theta_a)\sigma_c(\theta_c) - b\theta_a\theta_c = b\theta_a[\sigma_c(\theta_c) - \theta_c] = b\theta_a = A.\end{aligned}$$

Finally set $G := \text{Gal}(E/F)$.

Theorem 4.3. *Let $M := E(\theta_\delta, \theta_A, \theta_C, \theta_b)$. Then M/F is a Galois extension, M contains $F(\theta_a, \theta_b, \theta_c)$, and $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$.*

Proof. Let W^* be the \mathbb{F}_p -vector space in $E/\wp(E)$ generated by $[b]_E, [A]_E, [C]_E$ and $[\delta]_E$. Since

$$\begin{aligned}\sigma_c(\delta) &= \delta + A, \\ \sigma_a(\delta) &= \delta + C, \\ \sigma_a(A) &= A + b, \\ \sigma_c(C) &= C + b,\end{aligned}$$

we see that W^* is in fact an $\mathbb{F}_p[G]$ -module. Hence M/F is a Galois extension by Artin-Schreier theory.

Claim: $\dim_{\mathbb{F}_p}(W^*) = 4$. Hence $[L : F] = [L : E][E : F] = p^4 p^2 = p^6$.

Proof of Claim: From our hypothesis that $\dim_{\mathbb{F}_p}\langle [a]_F, [b]_F, [c]_F \rangle = 3$, we see that $\langle [b]_E \rangle \simeq \mathbb{F}_p$.

Clearly, $\langle [b]_E \rangle \subseteq (W^*)^G$. From the relation

$$[\sigma_a(A)]_E = [A]_E + [b]_E,$$

we see that $[A]_E$ is not in $(W^*)^G$. Hence $\dim_{\mathbb{F}_p}\langle [b]_E, [A]_E \rangle = 2$.

From the relation

$$[\sigma_c(C)]_E = [C]_E + [b]_E,$$

we see that $[C]_E$ is not in $(W^*)^{\sigma_c}$. But we have $\langle [b]_E, [A]_E \rangle \subseteq (W^*)^{\sigma_c}$. Hence

$$\dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E \rangle = 3.$$

Observe that the element $(\sigma_a - 1)(\sigma_c - 1)$ annihilates the $\mathbb{F}_p[G]$ -module $\langle [b]_E, [A]_E, [C]_E \rangle$, while

$$(\sigma_a - 1)(\sigma_c - 1)[\delta]_E = \sigma_a([A]_E) - [A]_E = [b]_E,$$

we see that

$$\dim_{\mathbb{F}_p} W^* = \dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E, [\delta]_E \rangle = 4.$$

Let $H^{a,b} = F(\theta_a, \theta_A, \theta_b)$ and $H^{b,c} = F(\theta_c, \theta_C, \theta_b)$. Let

$$N := H^{a,b}H^{b,c} = F(\theta_a, \theta_c, \theta_b, \theta_A, \theta_C) = E(\theta_b, \theta_A, \theta_C).$$

Then N/F is a Galois extension of degree p^5 . This is because $\text{Gal}(N/E)$ is dual to the $\mathbb{F}_p[G]$ -submodule $\langle [b]_E, [A]_E, [C]_E \rangle$ via Artin-Schreier theory, and the proof of the claim above shows that $\dim_{\mathbb{F}_p} \langle [b]_E, [A]_E, [C]_E \rangle = 3$. We have the following commutative diagram

$$\begin{array}{ccc} \text{Gal}(N/F) & \longrightarrow & \text{Gal}(H^{a,b}/F) \\ \downarrow & & \downarrow \\ \text{Gal}(H^{b,c}/F) & \longrightarrow & \text{Gal}(F(\theta_b)/F). \end{array}$$

So we have a homomorphism η from $\text{Gal}(N/F)$ to the pull-back $\text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\theta_b)/F)} \text{Gal}(H^{a,b}/F)$:

$$\eta: \text{Gal}(N/F) \longrightarrow \text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\theta_b)/F)} \text{Gal}(H^{a,b}/F),$$

which make the obvious diagram commute. We claim that η is injective. Indeed, let σ be an element in $\ker \eta$. Then $\sigma|_{H^{a,b}} = 1$ in $\text{Gal}(H^{a,b}/F)$, and $\sigma|_{H^{b,c}} = 1$ in $\text{Gal}(H^{b,c}/F)$. Since N is the compositum of $H^{a,b}$ and $H^{b,c}$, this implies that $\sigma = 1$, as desired.

Since $|\text{Gal}(H^{b,c}/F) \times_{\text{Gal}(F(\theta_b)/F)} \text{Gal}(H^{a,b}/F)| = p^5 = |\text{Gal}(N/F)|$, we see that η is actually an isomorphism. As in the proof of Proposition 4.1, we can choose an extension $\sigma_a \in \text{Gal}(H^{a,b}/F)$ of $\sigma_a \in \text{Gal}(F(\theta_a, \theta_b)/F)$ in such a way that

$$\sigma_a(\theta_A) = \theta_A + \theta_b.$$

Since the square commutative diagram above is a pull-back, we can choose an extension $\sigma_a \in \text{Gal}(N/F)$ of $\sigma_a \in \text{Gal}(H^{a,b}/F)$ in such a way that

$$\sigma_a|_{H^{b,c}} = 1.$$

Now we can choose any extension $\sigma_a \in \text{Gal}(M/F)$ of $\sigma_a \in \text{Gal}(N/F)$. Then we have

$$\sigma_a(\theta_A) = \theta_A + \theta_b \text{ and } \sigma_a|_{H^{b,c}} = 1.$$

Similarly, we can choose an extension $\sigma_c \in \text{Gal}(M/F)$ of $\sigma_c \in \text{Gal}(F(\theta_b, \theta_c)/F)$ in such a way that

$$\sigma_c(\theta_C) = \theta_C + \theta_b, \text{ and } \sigma_c|_{H^{a,b}} = 1.$$

We define $\sigma_b \in \text{Gal}(M/E)$ to be the element which is dual to $[b]_E$ via Artin-Schreier theory. In other words, we require that

$$\sigma_b(\theta_b) = 1 + \theta_b,$$

and σ_b acts trivially on θ_A, θ_C and θ_δ . We consider σ_b as an element in $\text{Gal}(M/F)$, then it is clear that σ_b is an extension of $\sigma_b \in \text{Gal}(F(\theta_a, \theta_b, \theta_c)/F)$. Let $W = \text{Gal}(M/E)$, and let $H = \text{Gal}(M/F)$, then we have the following exact sequence

$$1 \rightarrow W \rightarrow H \rightarrow G \rightarrow 1.$$

By Artin-Schreier theory, it follows that W is dual to W^* , and hence $W \simeq (\mathbb{Z}/p\mathbb{Z})^4$. In particular, we have $|H| = p^6$.

Recall that from [BD, Theorem 1], we know that the group $\mathbb{U}_4(\mathbb{F}_p)$ has a presentation with generators s_1, s_2, s_3 subject to the relations (R) displayed in the proof of Theorem 3.7. Note that $|\text{Gal}(M/F)| = p^6$. So in order to show that $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$, we shall show that σ_a, σ_b and σ_c generate $\text{Gal}(M/F)$ and they satisfy these relations (R). The proofs of the following claims are similar to the proofs of analogous claims in the proof of Theorem 3.7. Therefore we shall omit them.

Claim: The elements σ_a, σ_b and σ_c generate $\text{Gal}(M/F)$.

Claim: The order of σ_a is p .

Claim: The order of σ_b is p .

Claim: The order of σ_c is p .

Claim: $[\sigma_a, \sigma_c] = 1$.

Claim: $[\sigma_a, [\sigma_a, \sigma_b]] = [\sigma_b, [\sigma_a, \sigma_b]] = 1$.

Claim: $[\sigma_b, [\sigma_b, \sigma_c]] = [\sigma_c, [\sigma_b, \sigma_c]] = 1$.

Claim: $[[\sigma_a, \sigma_b], [\sigma_b, \sigma_c]] = 1$.

An explicit isomorphism $\varphi: \text{Gal}(M/F) \rightarrow \mathbb{U}_4(\mathbb{F}_p)$ may be defined as

$$\sigma_a \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_c \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

□

5. TRIPLE MASSEY PRODUCTS

Let G be a profinite group and p a prime number. We consider the finite field \mathbb{F}_p as a trivial discrete G -module. Let $\mathcal{C}^\bullet = (C^\bullet(G, \mathbb{F}_p), \partial, \cup)$ be the differential graded algebra of inhomogeneous continuous cochains of G with coefficients in \mathbb{F}_p (see [NSW, Ch. I, §2] and [MT1, Section 3]). For each $i = 0, 1, 2, \dots$, we write $H^i(G, \mathbb{F}_p)$ for the corresponding cohomology group. We denote by $Z^1(G, \mathbb{F}_p)$ the subgroup of $C^1(G, \mathbb{F}_p)$ consisting of all 1-cocycles. Because we use trivial action on the coefficients \mathbb{F}_p , we have $Z^1(G, \mathbb{F}_p) = H^1(G, \mathbb{F}_p) = \text{Hom}(G, \mathbb{F}_p)$. Let x, y, z be elements in $H^1(G, \mathbb{F}_p)$. Assume that

$$x \cup y = y \cup z = 0 \in H^2(G, \mathbb{F}_p).$$

In this case we say that the triple Massey product $\langle x, y, z \rangle$ is defined. Then there exist cochains a_{12} and a_{23} in $C^1(G, \mathbb{F}_p)$ such that

$$\partial a_{12} = x \cup y \quad \text{and} \quad \partial a_{23} = y \cup z,$$

in $C^2(G, \mathbb{F}_p)$. Then we say that $D := \{x, y, z, a_{12}, a_{23}\}$ is a *defining system* for the triple Massey product $\langle x, y, z \rangle$. Observe that

$$\begin{aligned} \partial(x \cup a_{23} + a_{12} \cup z) &= \partial x \cup a_{23} - x \cup \partial a_{23} + \partial a_{12} \cup z - a_{12} \cup \partial z \\ &= 0 \cup a_{23} - x \cup (y \cup z) + (x \cup y) \cup z - a_{12} \cup 0 \\ &= 0 \in C^2(G, \mathbb{F}_p). \end{aligned}$$

Therefore $x \cup a_{23} + a_{12} \cup z$ is a 2-cocycle. We define the value $\langle x, y, z \rangle_D$ of the triple Massey product $\langle x, y, z \rangle$ with respect to the defining system D to be the cohomology class $[x \cup a_{23} + a_{12} \cup z]$ in $H^2(G, \mathbb{F}_p)$. The set of all values $\langle x, y, z \rangle_D$ when D runs over the set of all defining systems, is called the triple Massey product $\langle x, y, z \rangle \subseteq H^2(G, \mathbb{F}_p)$. Note that we always have

$$\langle x, y, z \rangle = \langle x, y, z \rangle_D + x \cup H^1(G, \mathbb{F}_p) + H^1(G, \mathbb{F}_p) \cup z.$$

We also have the following result.

Lemma 5.1. *If the triple Massey products $\langle x, y, z \rangle$ and $\langle x, y', z \rangle$ are defined, then the triple Massey product $\langle x, y + y', z \rangle$ is defined, and*

$$\langle x, y + y', z \rangle = \langle x, y, z \rangle + \langle x, y', z \rangle.$$

Proof. Let $\{x, y, z, a_{12}, a_{23}\}$ (respectively $\{x, y', z, a'_{12}, a'_{23}\}$) be a defining system for $\langle x, y, z \rangle$ (respectively $\langle x, y', z \rangle$). Then $\{x, y + y', z, a_{12} + a'_{12}, a_{23} + a'_{23}\}$ is a defining system for $\langle x, y + y', z \rangle$. We also have

$$\begin{aligned} \langle x, y, z \rangle + \langle x, y', z \rangle &= [x \cup a_{23} + a_{12} \cup z] + x \cup H^1(G, \mathbb{F}_p) + H^1(G, \mathbb{F}_p) \cup z \\ &\quad + [x \cup a'_{23} + a'_{12} \cup z] + x \cup H^1(G, \mathbb{F}_p) + H^1(G, \mathbb{F}_p) \cup z \\ &= [x \cup (a_{23} + a'_{23}) + (a_{12} + a'_{12}) \cup z] + x \cup H^1(G, \mathbb{F}_p) + H^1(G, \mathbb{F}_p) \cup z \\ &= \langle x, y + y', z \rangle, \end{aligned}$$

as desired. \square

The following lemma is a special case of a well-known fact (see [Fe, Lemma 6.2.4 (ii)]) but for the sake of convenience we provide its proof.

Lemma 5.2. *If the triple Massey product $\langle x, y, z \rangle$ is defined, then for any $\lambda \in \mathbb{F}_p$ the triple Massey product $\langle x, \lambda y, z \rangle$ is defined, and*

$$\langle x, \lambda y, z \rangle \supseteq \lambda \langle x, y, z \rangle.$$

Proof. Let $D = \{x, y, z, a_{12}, a_{23}\}$ be any defining system for $\langle x, y, z \rangle$. Clearly $D' := \{x, \lambda y, z, \lambda a_{12}, \lambda a_{23}\}$ is a defining system for $\langle x, \lambda y, z \rangle$, and

$$\lambda \langle x, y, z \rangle_D = \lambda [x \cup a_{23} + a_{12} \cup z] = [x \cup (\lambda a_{23}) + (\lambda a_{12}) \cup z] = \langle x, \lambda y, z \rangle_{D'}.$$

Therefore $\lambda \langle x, y, z \rangle \subseteq \langle x, \lambda y, z \rangle$. \square

A direct consequence of Theorems 3.7, 3.9 and 4.3, is the following result which roughly says that every "non-degenerate" triple Massey product vanishes whenever it is defined.

Proposition 5.3. *Let F be an arbitrary field. Let χ_1, χ_2, χ_3 be elements in $\text{Hom}(G_F, \mathbb{F}_p)$. We assume that χ_1, χ_2, χ_3 are \mathbb{F}_p -linearly independent. If the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined, then it contains 0.*

Proof. Let L be the fixed field of $(F)^s$ under the kernel of the surjection $(\chi_1, \chi_2, \chi_3): G_F \rightarrow (\mathbb{F}_p)^3$. Then Theorems 3.7, 3.9 and 4.3 imply that L/F can be embedded in a Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extension M/F . Moreover there exist $\sigma_1, \sigma_2, \sigma_3$ in $\text{Gal}(M/F)$ such that they generate $\text{Gal}(M/F)$, and

$$\begin{aligned}\chi_1(\sigma_1) &= 1, \chi_1(\sigma_2) = 0, \chi_1(\sigma_3) = 0; \\ \chi_2(\sigma_1) &= 0, \chi_2(\sigma_2) = 1, \chi_2(\sigma_3) = 0; \\ \chi_3(\sigma_1) &= 0, \chi_3(\sigma_2) = 0, \chi_3(\sigma_3) = 1.\end{aligned}$$

(Note that for each $i = 1, 2, 3$, χ_i is trivial on $\text{Gal}(M/M_0)$, hence $\chi_i(\sigma_j)$ makes sense for every $j = 1, 2, 3$.) An explicit isomorphism $\varphi: \text{Gal}(M/F) \rightarrow \mathbb{U}_4(\mathbb{F}_p)$ can be defined as

$$\sigma_1 \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_2 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let ρ be the composite homomorphism $\rho: \text{Gal}_F \rightarrow \text{Gal}(M/F) \xrightarrow{\varphi} \mathbb{U}_4(\mathbb{F}_p)$. Then one can check that

$$\rho_{12} = \chi_1, \rho_{23} = \chi_2, \rho_{34} = \chi_3.$$

(Since all the maps $\rho, \chi_1, \chi_2, \chi_3$ factor through $\text{Gal}(M/F)$, it is enough to check these equalities on elements $\sigma_1, \sigma_2, \sigma_3$.) This implies that $\langle -\chi_1, -\chi_2, -\chi_3 \rangle$ contains 0 by [Dwy, Theorem 2.4]. Hence $\langle \chi_1, \chi_2, \chi_3 \rangle$ also contains 0. \square

For the sake of completeness we include the following proposition, which together with Proposition 5.3, immediately yields a full new proof for a result which was first proved by E. Matzri [Ma]. Matzri's result says that defined triple Massey products vanish over all fields containing a primitive p -th root of unity. Alternative cohomological proofs for Matzri's result are in [EMa2] and [MT5]. Our new proof given in this section of the crucial "non-degenerate" part of this result (see Proposition 5.3), which relies on explicit constructions of $\mathbb{U}_4(\mathbb{F}_p)$ -extensions, is a very natural proof because of Dwyer's result [Dwy, Theorem 2.4]. Observe that in [MT5] we extended this result to all fields.

Proposition 5.4. *Assume that $\dim_{\mathbb{F}_p} \langle [a]_F, [b]_F, [c]_F \rangle \leq 2$. Then if the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined, then it contains 0.*

Proof. We can also assume that a, b and c are not in $(F^\times)^p$. The case that $p = 2$, was treated in [MT1]. So we shall assume that $p > 2$.

Case 1: Assume that a and c are linearly dependent modulo $(F^\times)^p$. This case is considered in [MT5, Proof of Theorem 4.10]. We include a proof here for the convenience of the reader. Let $\varphi = \{\varphi_{ab}, \varphi_{bc}\}$ be a defining system for $\langle \chi_a, \chi_b, \chi_c \rangle$. We have

$$\begin{aligned} \text{res}_{\ker \chi_a}(\langle \chi_a, \chi_b, \chi_c \rangle_\varphi) &= \text{res}_{\ker \chi_a}(\chi_a \cup \varphi_{bc} + \varphi_{ab} \cup \chi_c) \\ &= \text{res}_{\ker \chi_a}(\chi_a) \cup \text{res}_{\ker \chi_a}(\varphi_{bc}) + \text{res}_{\ker \chi_a}(\varphi_{ab}) \cup \text{res}_{\ker \chi_a}(\chi_c) \\ &= 0 \cup \text{res}_{\ker \chi_a}(\varphi_{bc}) + \text{res}_{\ker \chi_a}(\varphi_{ab}) \cup 0 \\ &= 0. \end{aligned}$$

Then [Se1, Chapter XIV, Proposition 2], $\langle \chi_a, \chi_b, \chi_c \rangle_\varphi = \chi_a \cup \chi_x$ for some $x \in F^\times$. This implies that $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0.

Case 2: Assume that a and c are linearly independent. Then $[b]_F$ is in $\langle [a]_F, [c]_F \rangle$. Hence there exist $\lambda, \mu \in \mathbb{F}_p$ such that

$$\chi_b = \lambda \chi_a + \mu \chi_c.$$

Then we have

$$\langle \chi_a, \chi_b, \chi_c \rangle = \langle \chi_a, \lambda \chi_a, \chi_c \rangle + \langle \chi_a, \mu \chi_c, \chi_c \rangle \supseteq \lambda \langle \chi_a, \chi_a, \chi_c \rangle + \mu \langle \chi_a, \chi_c, \chi_c \rangle.$$

(The equality follows from Lemma 5.1 and the inequality follows from Lemma 5.2.) By [MT5, Theorem 5.9] (see also [MT5, Proof of Theorem 4.10, Case 2]), $\langle \chi_a, \chi_a, \chi_c \rangle$ and $\langle \chi_a, \chi_c, \chi_c \rangle$ both contain 0. Hence $\langle \chi_a, \chi_b, \chi_c \rangle$ also contains 0. \square

Theorem 5.5. *Let p be an arbitrary prime and F any field. Then the following statements are equivalent.*

- (1) *There exist χ_1, χ_2, χ_3 in $\text{Hom}(G_F, \mathbb{F}_p)$ such that they are \mathbb{F}_p -linearly independent, and if $\text{char} F \neq p$ then $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$.*
- (2) *There exists a Galois extension M/F such that $\text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$.*

Moreover, assume that (1) holds, and let L be the fixed field of $(F)^s$ under the kernel of the surjection $(\chi_1, \chi_2, \chi_3): G_F \rightarrow (\mathbb{F}_p)^3$. Then in (2) we can construct M/F explicitly such that L is embedded in M .

If F contains a primitive p -th root of unity, then the two above conditions are also equivalent to the following condition.

- (3) *There exist $a, b, c \in F^\times$ such that $[F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c}) : F] = p^3$ and $(a, b) = (b, c) = 0$.*

If F of characteristic p , then the two above conditions (1)-(2) are also equivalent to the following condition.

- (3') *There exist $a, b, c \in F^\times$ such that $[F(\theta_a, \theta_b, \theta_c) : F] = p^3$.*

Proof. The implication that (1) implies (2), follows from Theorems 3.7, 3.9 and 4.3.

Now assume that (2) holds. Let ρ be the composite $\rho: G_F \twoheadrightarrow \text{Gal}(M/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$. Let $\chi_1 := \rho_{12}$, $\chi_2 := \rho_{23}$ and $\chi_3 := \rho_{34}$. Then χ_1, χ_2, χ_3 are elements in $\text{Hom}(G_F, \mathbb{F}_p)$,

and $(\chi_1, \chi_2, \chi_3): G_F \rightarrow (\mathbb{F}_p)^3$ is surjective. This implies that χ_1, χ_2, χ_3 are \mathbb{F}_p -linearly independent by [MT4, Lemma 2.6].

On the other hand, since ρ is a group homomorphism, we see that

$$\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0.$$

Therefore (1) holds.

Now we assume that F contains a primitive p -th root of unity. Note that for any $a, b \in F^\times$, $\chi_a \cup \chi_b = 0$, if and only if $(a, b) = 0$ (see Subsection 2.1). Then (1) is equivalent to (3) by Kummer theory in conjunction with an observation that $[F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c}) : F] = p^3$, if and only if χ_a, χ_b, χ_c are \mathbb{F}_p -linearly independent.

Now we assume that F of characteristic $p > 0$. Then (1) is equivalent to (3') by Artin-Schreier theory in conjunction with an observation that $[F(\theta_a, \theta_b, \theta_c) : F] = p^3$, if and only if χ_a, χ_b, χ_c are \mathbb{F}_p -linearly independent. \square

REFERENCES

- [Alb] A. A. Albert, *Modern Higher Algebra*, University of Chicago Press, Chicago, 1937.
- [AS] S. A. Amitsur and D. Saltman, *Generic abelian crossed products and p -algebras*, J. Algebra 51 (1) (1978), 76-87.
- [ASch] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Univ. Hamburg 5 (1927) pp. 225-231. Reprinted in: Artin's Collected Papers (Eds. S. Lang and J. Tate), Springer-Verlag, New York, 1965, pp. 289-295.
- [BD] D. K. Biss and S. Dasgupta, *A presentation for the unipotent group over rings with identity*, J. Algebra 237 (2001), 691-707.
- [BT1] F. Bogomolov and Y. Tschinkel, *Reconstruction of higher-dimensional function fields*, Moscow Math. Journal 11, no. 2 (2011), 185-204.
- [BT2] F. Bogomolov and Y. Tschinkel, *Introduction to birational anabelian geometry*, Current developments in algebraic geometry, 17-63, Math. Sci. Res. Inst. Publ., 59, Cambridge Univ. Press, Cambridge, 2012.
- [Co] I. G. Connell, *Elementary generalizations of Hilbert's theorem 90*, Canad. Math. Bull. 8 (1965), 749-757.
- [CEM] S. K. Chebolu, I. Efrat and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. 352 (2012), no. 1, 205-221.
- [CMS] S. K. Chebolu, J. Mináč and A. Schultz, *Galois p -groups and Galois modules*, to appear in Rocky Mountain J. Math., arXiv:1411.6495.
- [DGMS] P. Deligne, P. Griffiths, J. Morgan and D. Sullivan, *Real homotopy theory of Kähler manifolds*, Invent. Math. 29 (1975), 245-274.
- [DMSS] R. Dwilewicz, J. Mináč, A. Schultz and J. Swallow, *Hilbert 90 for biquadratic extensions*, American Mathematical Monthly 114 (7) (2007), 577-587.
- [Dwy] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra 6 (1975), no. 2, 177-190.
- [Ef] I. Efrat, *The Zassenhaus filtration, Massey products, and representations of profinite groups*, Adv. Math. 263 (2014), 389-411.
- [EMa1] I. Efrat and E. Matzri, *Vanishing of Massey products and Brauer groups*, Can. Math. Bull. 58 (2015), 730-740.

- [EMa2] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, to appear in J. Eur. Math. Soc., arXiv:1412.7265.
- [EM1] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. 133 (2011), no. 6, 1503-1532.
- [EM2] I. Efrat and J. Mináč, *Galois groups and cohomological functors*, to appear in Trans. Amer. Math. Soc., DOI:http://dx.doi.org/10.1090/tran/6724, arXiv:1103.1508v1.
- [Fe] R. Fenn, *Techniques of Geometric Topology*, London Math. Soc. Lect. Notes 57, Cambridge 1983.
- [Ga] J. Gärtner, *Higher Massey products in the cohomology of mild pro- p -groups* J. Algebra 422 (2015), 788-820.
- [GLMS] W. Gao, D. Leep, J. Mináč and T. L. Smith, *Galois groups over nonrigid fields*, Proceedings of the International Conference on Valuation Theory and its Applications, Vol. II (Saskatoon, SK, 1999), 61-77, Fields Inst. Commun., 33, Amer. Math. Soc., Providence, RI, 2003.
- [GS] H. G. Grundman and T. L. Smith, *Galois realizability of groups of order 64*, Cent. Eur. J. Math. 8(5) (2010), 846-854.
- [Ha] M. Hall, *The Theory of Groups*, The Macmillan Company, New York, 1963.
- [HW] M. Hopkins and K. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra 219 (2015), 1304-1319.
- [Je] C. U. Jensen, *Finite groups as Galois groups over arbitrary fields*, Proceedings of the International Conference on Algebra, Part 2 (Novosibirsk, 1989) Contemp. Math., vol. 131, Amer. Math. Soc., Providence, RI, 1992, pp. 435-448.
- [JLY] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, MSRI Publications Volume 45, Cambridge University Press, 2002.
- [Ko] H. Koch, *Galois theory of p -extensions*, Springer Monographs in Mathematics (2001).
- [La] J. Labute, *Linking Numbers and the Tame Fontaine-Mazur Conjecture*, Ann. Math. Québec (2014), 38: 61-71.
- [M] R. Massy, *Construction de p -extensions galoisiennes d'un corps de caractéristique différente de p* , J. Algebra 109 (1987), no. 2, 508-535.
- [MN_g] R. Massy, and T. Nguyen-Quang-Do, *Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale*, J. Reine Angew. Math. 291 (1977), 149-161.
- [Ma] E. Matzri, *Triple Massey products in Galois cohomology*, preprint (2014), arXiv:1411.4146.
- [McL] C. McLeman, *p -tower groups over quadratic imaginary number fields*, Ann. Sci. Math. Québec 32 (2008), no. 2, 199-209.
- [Me] A. S. Merkurjev, *Certain K -cohomology groups of Severi-Brauer varieties*, Proc. Symp. Pure Math. 58.2 (1995), 319-331.
- [Mi1] I. M. Michailov, *Four non-abelian groups of order p^4 as Galois groups*, J. Algebra 307 (2007), 287-299.
- [Mi2] I. M. Michailov, *Galois realizability of groups of orders p^5 and p^6* , Cent. Eur. J. Math. 11(5) (2013), 910-923.
- [MZ] I. M. Michailov and N. P. Ziapkov, *On realizability of p -groups as Galois groups*, Serdica Math. J. 37 (2011), 173-210.
- [MSp] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. of Math. (2) 144 (1996), no. 1, 35-60.
- [MS1] J. Mináč and J. Swallow, *Galois module structure of p th-power classes of extensions of degree p* , Israel J. Math. 138 (2003), 29-42.
- [MS2] J. Mináč and J. Swallow, *Galois embedding problems with cyclic quotient of order p* , Israel J. Math. 145 (2005), 93-112.
- [MSS] J. Mináč, A. Schultz and J. Swallow, *Automatic realizations of Galois groups with cyclic quotient of order p^n* , J. Théor. Nombres Bordeaux 20 (2008), no. 2, 419-430.
- [MT1] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, to appear in J. Eur. Math. Soc., arXiv:1307.6624.

- [MT2] J. Mináč and N. D. Tân, *The Kernel Unipotent Conjecture and Massey products on an odd rigid field* (with an appendix by I. Efrat, J. Mináč and N. D. Tân), *Adv. Math.* 273 (2015), 242-270.
- [MT3] J. Mináč and N. D. Tân, *Triple Massey products over global fields*, *Doc. Math* 20 (2015) 1467-1480.
- [MT4] J. Mináč and N. D. Tân, *Counting Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions using Massey products*, preprint(2014), arXiv:1408.2586.
- [MT5] J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, to appear in *J. London Math. Soc.*, arXiv:1412.7611.
- [NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, 323, Springer-Verlag, Berlin, 2000.
- [NQD] T. Nguyen Quang Do, *Étude Kummerienne de la q -suite centrale descendante d'un group de Galois*, *Publ. Math. Besançon. Algèbre et théorie des nombres*, vol. 2012/2, Presses Univ. Franche-Comté, Besançon, 2012, 123-139.
- [Pop] F. Pop, *On the birational anabelian program initiated by Bogomolov I*, *Invent. Math.* 187 (2012), no. 3, 511-533.
- [Sch] A. Schultz, *Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p -abelian kernel*, *J. Algebra* 411 (2014), 50-91.
- [Se1] J.-P. Serre, *Local fields*, translated from the French by M. J. Greenberg, *Graduate Texts in Mathematics*, 67, Springer-Verlag, New York-Berlin, 1979.
- [Se2] J.-P. Serre, *Galois cohomology*, translated from the French by P. Ion and revised by the author, corrected reprint of the 1997 English edition, *Springer Monographs in Mathematics*, Springer-Verlag, Berlin, 2002.
- [Se3] J.-P. Serre, *Topics in Galois Theory*, Second edition, *Research Notes in Mathematics*, vol. 1, A K Peters Ltd., Wellesley, MA, 2008. With notes by Henri Darmon.
- [Sha] R. Sharifi, *Twisted Heisenberg representations and local conductors*, Ph.D. thesis, The University of Chicago (1999).
- [Vi] F. R. Villegas, *Relations between quadratic forms and certain Galois extensions*, a manuscript, Ohio State University, 1988, <http://www.math.utexas.edu/users/villegas/osu.pdf>.
- [Voe1] V. Voevodsky, *Motivic cohomology with $\mathbb{Z}/2$ -coefficients*, *Publ. Math. Inst. Hautes Études Sci.* No. 98 (2003), 59-104.
- [Voe2] V. Voevodsky, *On motivic cohomology with \mathbb{Z}/l -coefficients*, *Ann. of Math. (2)* 174 (2011), no. 1, 401-438.
- [Wat] W. C. Waterhouse, *The normal closures of certain Kummer extensions*, *Canad. Math. Bull.* 37 (1994), no. 1, 133-139.
- [Wh] G. Whaples, *Algebraic extensions of arbitrary fields*, *Duke Math. J.* 24 (1957), 201- 204.
- [Wi] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f* , *J. Reine Angew. Math.* 174 (1936), 237-245.
- [Za] H. Zassenhaus, *The Theory of Groups*, Chelsea Publishing Company, 1949.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
E-mail address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
 AND INSTITUTE OF MATHEMATICS, VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY, 18 HOANG
 QUOC VIET, 10307, HANOI - VIETNAM
E-mail address: duytan@math.ac.vn